SSP Secrets

Foundation for CMMC Assessment

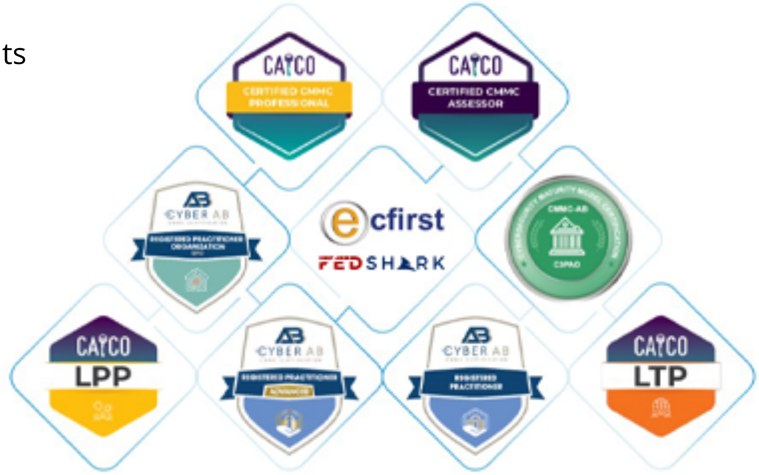
Uday Ali Pabrai & Josh Williams

Global AI Cyber Defence Thought Leaders

Topics

- Background: Why CMMC?
- CMMC Level 1 Fundamentals
- CMMC Level 1 Domains and Requirements
- CMMC Assessment Terminology
- CMMC Assets
- Level 1 Scoping
- Level 1 Assessment Findings & Results
- Level 1 Compliance Affirmation
- Level 1 Readiness Checklist
- Sample Level 1 Report Findings
- Conclusion

The DoD CMMC Ecosystem



AI Defense, *Beyond Cyber*

The U.S. Defense Industrial Base (DIB) sector is under attack. It has been, is, and will continue to be attacked by threat actors of all stripes, including nation-state threat actors and their affiliates. The DIB represents the supply chain of the Department of Defense (DoD) — hence the Cybersecurity Maturity Model Certification (CMMC) standard from the DoD to secure the supply chain. Stated another way, CMMC is an uber-ATO (Authorization To Operate) for the DIB that is intended to cultivate and maintain resilience in the DoD supply chain.

CMMC is organized into three Levels, and the security requirements increase from Level 1 to Level 3. Our focus in this brief is to guide organizations to understand and be prepared to address CMMC Level 1 requirements.

The objective of CMMC Level 1 is to secure Federal Contract Information (FCI). FCI is information provided by or generated for the U.S. government under contract not intended for public release. CMMC Level 1 encompasses the *basic safeguarding requirements* for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21.

In this brief, we:

- Understand CMMC Level 1 fundamentals, including associated Domains and Requirements
- Examine CMMC Assessment terminology
- Identify Asset categories and their impact on a CMMC Level 1 Assessment
- Review CMMC Level 1 Scoping, including scenarios
- Step through CMMC Level 1 Finding Criteria
- Analyze a checklist for CMMC Level 1 Assessment readiness

Background: Why CMMC?

The DIB is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The DIB sector consists of over 300,000 companies across the United States and globally.

The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain undercuts U.S. technical advantages and innovation as well as significantly increases the risk to national security.

CMMC has been designed to provide assurance to the DoD that a DIB contactor can adequately protect Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. When implementing the CMMC model, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s), depending on where the information to be protected is handled and stored.

The CMMC framework is coupled with a certification program to verify the implementation of requirements by the DIB — hence the requirement for a CMMC assessment to determine certification requirements are met.

CMMC Level 1 Fundamentals

CMMC Level 1 focuses on the protection of FCI which is defined in 32 CFR § 170.4 and 48 CFR § 4.1901and consists of the 15 basic safeguarding requirements specified in FAR Clause 52.204-21.

> FCI is 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.

Assessment objectives are provided for each Level 1 requirement and are based on existing criteria in NIST SP 800-171A, modified for FCI rather than CUI, as set forth in 32 CFR § 170.15(c)(1)(i). The criteria are authoritative and provide the basis for the self-assessment of a requirement.

CMMC Level 1 Domains and Requirements

CMMC Level 1 includes six Domains and fifteen requirements. The six Level 1 Domains are:

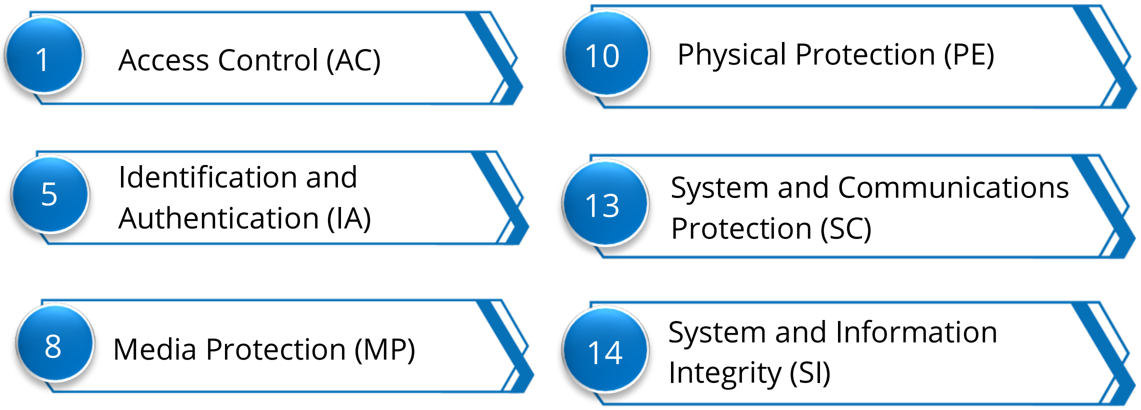

1
Access Control (AC)
10
Physical Protection (PE)
5
Identification and Authentication (IA)
13
System and Communications Protection (SC)
8
Media Protection (MP)
14
System and Information Integrity (SI)

Figure 1: CMMC Level 1 Domains.

CMMC Level 1 is about protection of FCI across six Domains and fifteen requirements. It is about basic safeguarding requirements specified in FAR Clause 52.204-21.

CMMC Level 1 includes fifteen (15) requirements across these six Domains. All of the requirements are applicable to FCI data.

#	Domains	Requirements
1	Access Control (AC)	1. Authorized Access Control (AC.L1-b.1.i)
		2. Transaction & Function Control (AC.L1-b.1.ii)
		3. External Connections (AC.L1-b.1.iii)
		4. Control Public Information (AC.L1-b.1.iv)
2	Identification and Authentication (IA)	5. Identification (IA.L1-b.1.v)
		6. Authentication (IA.L1-b.1.vi)
3	Media Protection (MP)	7. Media Disposal (MP.L1-b.1.vii)
4	Physical Protection (PE)	8. Limit Physical Access (PE.L1-b.1.viii)
		9. Manage Visitors & Physical Access (PE.L1-b.1.ix)
5	System and Communications Protection (SC)	10. Boundary Protection (SC.L1-b.1.x)
		11. Public-Access System Separation (SC.L1-b.1.xi)
6	System and Information Integrity (SI)	12. Flaw Remediation (SI.L1-b.1.xii)
		13. Malicious Code Protection (SI.L1-b.1.xiii)
		14. Update Malicious Code Protection (SI.L1-b.1.xiv)
		15. System & File Scanning (SI.L1-b.1.xv)

Figure 2: CMMC Level 1 Requirements.

CMMC Level 1 Assessment Objectives

#	Domains	Requirements	Assessment Objectives
1	Access Control (AC)	1. Authorized Access Control (AC.L1-b.1.i)	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. [f] System access is limited to authorized devices (including other systems).
		2. Transaction & Function Control (AC.L1-b.1.ii)	Determine if: [a] The types of transactions and functions that authorized users are permitted to execute are defined. [b] System access is limited to the defined types of transactions and functions for authorized users.
		3. External Connections (AC.L1-b.1.iii)	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. [f] The use of external systems is controlled/limited.
		4. Control Public Information (AC.L1-b.1.iv)	Determine if: [a] Individuals authorized to post or process information on publicly accessible systems are identified.

#	Domains	Requirements	Assessment Objectives
			[b] Procedures to ensure FCI is not posted or processed on publicly accessible systems are identified. [c] A review process is in place prior to posting any content to publicly accessible systems. [d] Content on publicly accessible systems is reviewed to ensure that it does not include FCI. [e] Mechanisms are in place to remove and address improper posting of FCI.
2	Identification and Authentication (IA)	5. Identification (IA.L1-b.1.v)	Determine if: [a] System users are identified. [b] Processes acting on behalf of users are identified. [c] Devices accessing the system are identified.
		6. Authentication (IA.L1-b.1.vi)	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. [c] The identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.
3	Media Protection (MP)	7. Media Disposal (MP.L1-b.1.vii)	Determine if: [a] System media containing FCI is sanitized or destroyed before disposal. [b] System media containing FCI is sanitized before it is released for reuse.
4	Physical Protection (PE)	8. Limit Physical Access (PE.L1-b.1.viii)	Determine if: [a] Authorized individuals allowed physical access are identified. [b] Physical access to organizational systems is limited to authorized individuals.

#	Domains	Requirements	Assessment Objectives
			[c] Physical access to equipment is limited to authorized individuals. [d] Physical access to operating environments is limited to authorized individuals.
		9. Manage Visitors & Physical Access (PE.L1-b.1.ix)	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. [f] Physical access devices are managed.
5	System and Communications Protection (SC)	10. Boundary Protection (SC.L1-b.1.x)	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. [h] Communications are protected at key internal boundaries.
		11. Public-Access System Separation (SC.L1-b.1.xi)	Determine if: [a] Publicly accessible system components are identified. [b] Subnetworks for publicly accessible system components are physically or logically separated from internal networks.
6	System and Information Integrity (SI)	12. Flaw Remediation (SI.L1-b.1.xii)	Determine if: [a] The time within which to identify system flaws is specified.

#	Domains	Requirements	Assessment Objectives
			[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. [f] System flaws are corrected within the specified time frame.
		13. Malicious Code Protection (SI.L1-b.1.xiii)	Determine if: [a] Designated locations for malicious code protection are identified. [b] Protection from malicious code at designated locations is provided.
		14. Update Malicious Code Protection (SI.L1-b.1.xiv)	Determine if: [a] Malicious code protection mechanisms are updated when new releases are available.
		15. System & File Scanning (SI.L1-b.1.xv)	Determine if: [a] The frequency for malicious code scans is defined. [b] Malicious code scans are performed within the defined frequency. [c] Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Figure 3: CMMC Level 1 Domains, Requirements and Assessment Objectives.

CMMC Assessment Terminology

Let us examine key terminology associated with CMMC Assessment Level 1.

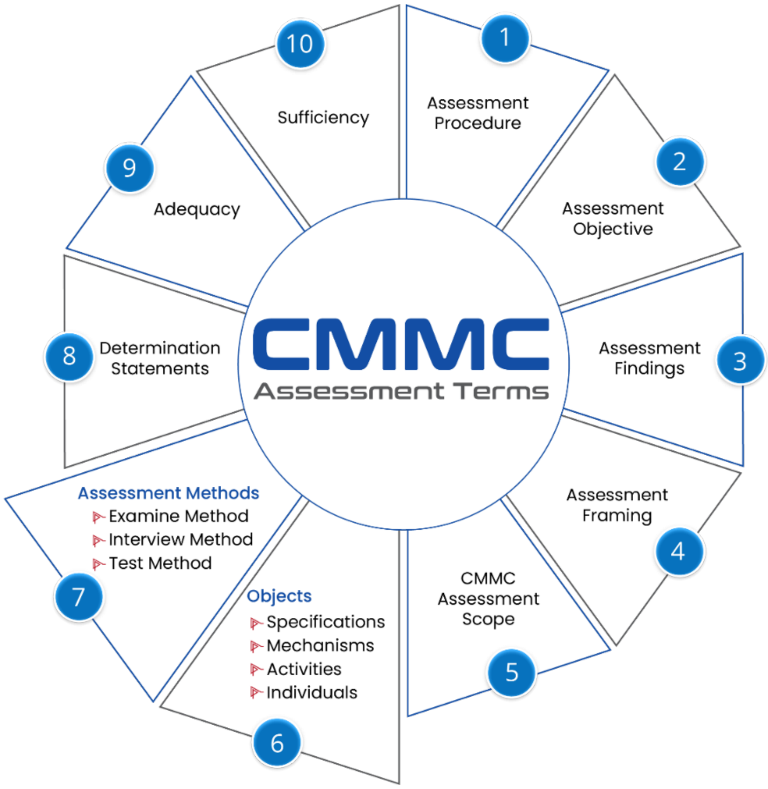


Figure 4: CMMC Assessment Terminology.

Assessment Procedure

The assessment procedure consists of an assessment objective and a set of potential assessment methods and assessment objects that can be used to conduct the assessment.

Assessment Procedure =
Assessment Objective + Assessment Methods + Assessment Objects

Assessment Objective

Each assessment objective includes a determination statement related to the requirement that is the subject of the assessment.

Assessment Findings

The application of an assessment procedure to a requirement produces assessment findings. These findings reflect, or are subsequently used, to help determine if the requirement has been satisfied.

Assessment Framing

Framing is the requirement of identifying the size, scale, date, time, place, manner, resources, and level of effort associated with the prospective conduct of a CMMC Assessment. High-level contract framing is performed jointly by the Certified Third-Party Assessor Organization (C3PAO) and the Organization Seeking Certification (OSC) and is conducted at the beginning of the assessment.

CMMC Assessment Scope

This describes the boundaries within an organization's networked environment that contain all the assets that will be assessed. CMMC Assessment Scope is initially determined by the OSC and then validated by the C3PAO.

Assessment Objects

The assessment objects identify the specific items being assessed and can include,

Specifications
Mechanisms
Activities
Individuals

Figure 5: CMMC Assessment Objects.

The assessment objects can be documents, mechanisms, or activities in final form; drafts of policies or documentation are not eligible to be used as evidence because they are not yet official and are still subject to change.

<u>Specifications</u>

Specifications are the document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, and architectural designs) associated with a system.

> An artifact is what can be examined (reviewing, inspecting, observing, studying, or analyzing).

Mechanisms

Mechanisms are the specific hardware, software, or firmware safeguards employed within a system.

Activities

Activities are the protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan, and monitoring network traffic).

Individuals

Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities.

Assessment Methods

The assessment methods define the nature and the extent of the assessor's actions. Assessment methods include:

Figure 6: Assessment Methods.

Examine Method

The examine method is the process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence.

Interview Method

The interview method is the process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.

Test Method

The test method is the process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.

Interviews tell what the OSA staff believe to be true, documentation provides **evidence** of implementing policies and procedures, and **testing** demonstrates what has or has not been done.

Determination Statements

The determination statements are linked to the content of the requirement to ensure traceability of the assessment results to the requirements.

Using the three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

Adequacy

Criterion will determine if a given artifact, interview response (affirmation), demonstration, or test meets the CMMC requirement.

Adequacy answers the question.
Does the Assessment Team have the right evidence?

Sufficiency

Criteria is needed to verify, based on Assessment and organizational scope, that coverage by domain, requirement and Host Units, Supporting Units, and enclaves is enough (sufficient) to rate against each requirement by the process role performing the work.

Sufficiency answers the question.
Does the Assessment Team have enough of the right evidence?

CMMC Level 1 Terms

The terms specifically associated with CMMC Level 1 include:

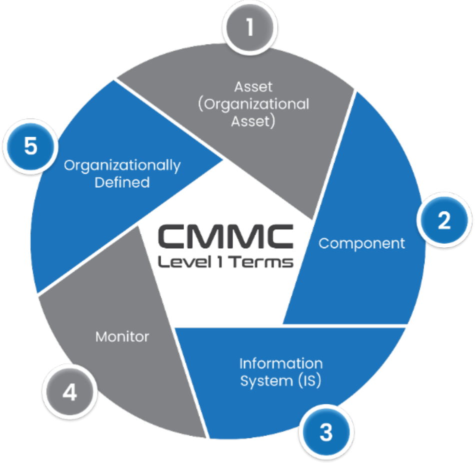


Figure 7: CMMC Level 1 Terms.

Asset (Organizational Asset)
An asset is anything that has value to an organization, including but not limited to another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). Understanding assets is critical to identifying the CMMC Assessment Scope.

Component
A component is a discrete, identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware. A component is one type of asset.

Information System (IS)
An Information System is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. An IS is one type of asset.

Monitor
Monitoring involves continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected.

Organizationally Defined
As determined by the OSA being assessed, except as defined in the case of Organization-Defined Parameter (ODP). This can be applied to a frequency or rate at which something occurs within a given time period, or it could be associated with describing the configuration of an OSA's solution.

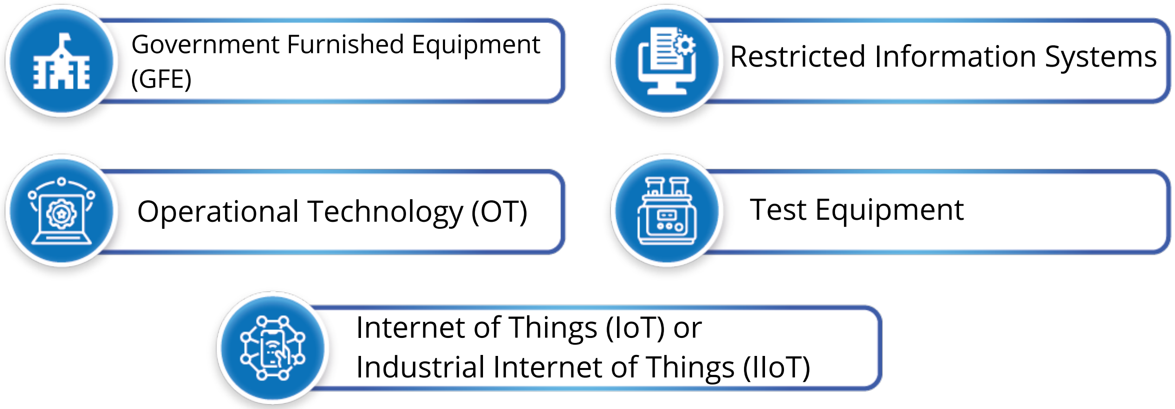
CMMC Assets

The CMMC Assessment Scope defines which assets within the OSA's environment will be assessed. CMMC defines five asset categories for scoping activities. These asset categories are:

1. CUI Assets
2. Security Protection Assets
3. Contractor Risk Managed Assets
4. Specialized Assets
5. Out-of-Scope Assets

CUI Assets process, store or transmit CUI. *Security Protection Assets* provide security functions or capabilities to the OSA's CMMC Assessment Scope. *Contractor Risk Managed Assets* are capable of, but are not intended to process, store, or transmit CUI because of the security policy, procedures, and requirements in place.

Specialized Assets for CMMC include:



Government Furnished Equipment (GFE)

Restricted Information Systems

Operational Technology (OT)

Test Equipment

Internet of Things (IoT) or Industrial Internet of Things (IIoT)

Figure 8: Specialized Assets for CMMC.

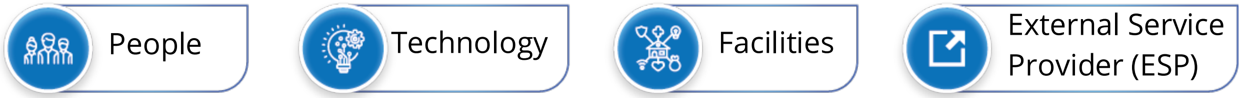
Out-of-Scope Assets cannot process, store, or transmit CUI, and do not provide security protections for CUI Assets. Assets that are physically or logically separated from CUI Assets and do not provide security protections for CUI Assets are also Out-of-Scope Assets.

Level 1 Scoping

Self-Assessment is the term used by CMMC for the activity performed by a DIB contractor to evaluate their own CMMC Level. The OSC is the entity going through the CMMC assessment process to receive a level of certification for a given environment.

For a CMMC Level 1 Self-Assessment, the assets that process, store, or transmit FCI are considered in-scope and should be assessed against the CMMC Level 1 requirements.

To appropriately scope a CMMC Level 1 Self-Assessment, the contractor should consider:



People

Technology

Facilities

External Service Provider (ESP)

Figure 9: CMMC Level 1 Self-Assessment.

within their environment that process, store or transmit FCI. Assets that process, store, or transmit FCI are considered in the Self-Assessment Scope.

From the perspective of the CMMC standard, there are a few key terms that must be understood from an assessment scope perspective. These terms are:

- HQ Organization
- Host Unit
- Supporting Organization
- Enclave

Headquarter (HQ) Organization is the legal entity that will be delivering services or products under the terms of a DoD contract. The HQ Organization itself could be the OSC, or it could designate a Host Unit as the OSC.

Host Unit is the part of the company being assessed and considered the OSC for purposes of the CMMC Assessment. A Host Unit could be a location, division, product line, or any other logical segmentation of an organization that can be independently assessed. Assessment results will be codified with the Host Unit name.

The HQ Organization, and in some cases the OSC, will register in SAM.gov and be issued an UEI and CAGE code. The Assessment cannot proceed if the OSC does not have a CAGE code.

Unique Entity ID (UEI)

Commercial And Government Entity (CAGE)

Supporting Organization is a logical organizational boundary that is supporting the Host Unit or enclave being assessed. Though not part of the logical segmentation, systems or people within the Supporting Unit may still have access to CUI or FCI, so therefore must be included within the scope of the Assessment.

Enclave refers to a set of system resources that operate within the same security domain and share the protection of a single, common, and continuous security perimeter. An enclave is a segmentation of an organization's network or data that is intended to "wall off" that network or database from all other networks or systems.

A CMMC Assessment can be within the Assessment Scope of an enclave.

CMMC Level 1 requirements may apply to an entire enterprise infrastructure or to a particular enclave(s), depending upon where the FCI will be processed, stored, or transmitted.

OSAs can choose to perform the annual Self-Assessment internally or engage a third party to assist. Use of a third party to assist is still considered a Self-Assessment and does not result in certification.

Before an assessment can begin, the OSC must specify the CMMC Self-Assessment Scope. The Scope informs which assets within the contractor's environment will be assessed and details of the Self-Assessment. In-Scope Assets are part of the CMMC Assessment Scope and are assessed against all CMMC Level 1 requirements.

Level 1 Scenarios

Consider the following two scenarios which inform how the contractor satisfies the CMMC Level 1 requirement.

Scenario 1

When the contractor considers all its technology and ESPs, it will convey how they satisfy the following requirements:

- AC.L1-b.1.iii — Verify and control/limit connections to and use of external information systems.
- SC.L1-b.1.x — 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.

Scenario 2

Identifying the people within the contractor's organization that process, store, or transmit FCI, informs how that contractor performs the following requirement:

- IA.L1-b.1.v, Identify information system users, processes acting on behalf of users, or devices.

Level 1 Assessment Findings & Results

The Self-Assessment of a CMMC requirement results in one of three possible findings:

- MET
- NOT MET
- NOT APPLICABLE

MET

All applicable objectives for the security requirement are satisfied based on evidence. All evidence must be in final form and not draft. Unacceptable forms of evidence include working papers, drafts, and unofficial or unapproved policies. For each security requirement marked MET, it is best practice to record statements that indicate the response conforms to all objectives and document the appropriate evidence to support the response.

NOT MET

One or more objectives of the security requirement is not satisfied. For each security requirement marked NOT MET, it is best practice to record statements that explain why and document the appropriate evidence showing that the OSA does not conform fully to all of the objectives.

NOT APPLICABLE (N/A)

A security requirement and/or objective does not apply at the time of the assessment. For each security requirement marked N/A, it is best practice to record a statement that explains why the requirement does not apply to the OSA.

For example, SC.L1-b.1.xi – Public-Access System Separation, might be N/A if there are no publicly accessible systems.

Evidence types include artifacts (examine), interview (affirmation), and test (demonstration or observation).

Level 1 Compliance Affirmation

CMMC Level 1 Self-Assessment requirements are set forth in 32 CFR § 170.15. The OSA will assess its own contractor information system(s) to determine if it meets all the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21. OSAs should use the self-assessment methods as described in 32 CFR § 170.15.

Level 1 Readiness Checklist

Certification Assessment Readiness Review (CA-RR) Checklist
Let us review a Readiness Checklist for a CMMC Level 1 Assessment.

#	Readiness Checklist	Status
1	**Attendees**	
2	**Analyze Assessment Requirements**	
	Assessment Framing	
	CMMC Assessment Scope	
3	**Evaluating Evidence Non-Duplication**	
4	**Evidence Readiness**	
	Artifacts	
	Interviews	
	Examine/Test(s) Schedule	
5	**OSC Assessment Readiness**	
6	**Identify Resources and Schedule**	
	On-site Assessment	
	Hybrid Assessment (Virtual (Collaboration Tool) & On-site))	
	Virtual Assessment	
7	**Identify and Manage Assessment Risks**	
	Personnel	
	Logistics	
	Facilities	
	Schedule	
	Cost	
	Data	
8	**Assessment Approval**	
	Affirmation Letter from Senior Executives	
	Upload Self-Assessment	

Figure 10: Level 1 Readiness Checklist.

Sample Level 1 Report Findings

We now review an example of findings related to a CMMC Level 1 Assessment.

#	Domain	Requirements	Status
1	Access Control (AC)	1. Authorized Access Control (AC.L1-b.1.i)	Met
		2. Transaction & Function Control (AC.L1-b.1.ii)	Met
		3. External Connections (AC.L1-b.1.iii)	Met
		4. Control Public Information (AC.L1-b.1.iv)	Met
2	Identification and Authentication (IA)	5. Identification (IA.L1-b.1.v)	Met
		6. Authentication (IA.L1-b.1.vi)	Met
3	Media Protection (MP)	7. Media Disposal (MP.L1-b.1.vii)	Met
4	Physical Protection (PE)	8. Limit Physical Access (PE.L1-b.1.viii)	Met
		9. Manage Visitors & Physical Access (PE.L1-b.1.ix)	Met
5	System and Communications Protection (SC)	10. Boundary Protection (SC.L1-b.1.x)	Met
		11. Public-Access System Separation (SC.L1-b.1.xi)	Met
6	System and Information Integrity (SI)	12. Flaw Remediation (SI.L1-b.1.xii)	Met
		13. Malicious Code Protection (SI.L1-b.1.xiii)	Met
		14. Update Malicious Code Protection (SI.L1-b.1.xiv)	Met
		15. System & File Scanning (SI.L1-b.1.xv)	Met

Figure 11: Sample Level 1 Report Findings.

Conclusion

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. Because different self-assessment objectives can be met in different ways (e.g., through documentation, computer configuration, network configuration, or training), a variety of techniques may be used to determine if the OSA meets the Level 1 requirements, including any of the three assessment methods from NIST SP 800-171A.

Organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results).

The OSA will assess its own contractor information system(s) to determine if it meet all the basic safeguarding requirements for FCI specified in FAR Clause 52.204-21. OSAs should use the self-assessment methods as described in 32 CFR § 170.15.

Organizations [OSAs] are not expected to employ all assessment methods and objects contained within the assessment procedures identified. This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the [FCI] requirements have been satisfied.

CMMC Level 1 requirements may apply to an entire enterprise infrastructure or to a particular enclave(s), depending upon where the FCI will be processed, stored, or transmitted.

OSAs can choose to perform the annual self-assessment internally or engage a third party to assist. Use of a third party to assist is still considered a self-assessment and does not result in a certification.

Global AI Cyber Defense Thought Leader

MSEE | CISSP (ISSAP | ISSMP) | CMMC (CCA, CCP, PA, PI, RPA, RP) | HITRUST® CCSFP | Security+

ISACA TOP-RATED SPEAKER ★★★★★

Mr. Ali Pabrai, a global AI cybersecurity & compliance expert, is the chairman & chief executive of ecfirst. A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide. His career was launched with the U.S. Department of Energy's nuclear research facility, Fermi National Accelerator Laboratory. He has served as vice chairman and in several senior officer positions with NASDAQ-based firms.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, CMMC, GDPR, CCPA, FERPA, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations.

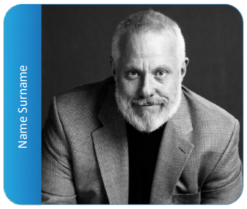
Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Bahrain, Jordan, South Africa, Egypt, Ghana and other countries.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the U.S. Defense Intelligence Agency (DIA), and the U.S. Naval Surface Warfare Center.

Mr. Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

U.S. Department of Defense CMMC Program
CYBER AB
REGISTERED PRACTITIONER
CYBER AB
REGISTERED PRACTITIONER ADVANCED
CAICO CERTIFIED CMMC PROFESSIONAL
CAICO CERTIFIED CMMC ASSESSOR

> "We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years - with one unanimous word that keeps resounding among audiences and staff alike - AWESOME!"
> **Michael Mach** | *Conference Program Manager* | *ISACA*



A cyber security practitioner with strong technical and leadership experience in both the public and private sectors, including information warfare engagements against GSFG, the Pakistani Hackers Club, the Chinese Communist Party, and Russia-affiliate BlackCat/ALPHV.

Classified and unclassified publication credits, including for NSF Award ACI-1626338 with Oak Ridge National Laboratory. Currently senior SME for regional healthcare network comprising 32 hospitals, 700 sites of care, multiple health centers, physician practices, rehab locations and other outpatient care locations in eastern Pennsylvania and NJ; implemented first private Full Operating Capability of the MITRE ATT&CK Framework for threat hunting. Most recently, Vice President of Security for a global IT Infrastructure Solutions, Data Storage and Cloud Services firm headquartered in the Fort Meade, MD area.

Provided subject matter expertise and multi-source fusion for incidence response and remediation including against the nation-state maleficent Yu Pingan responsible for the OPM breach. Created and operationalized a Cybersecurity Apprenticeship Program. Prior, managing principal of a DC-area management-consulting firm which crafted the first ever HIGH baseline for FedRAMP. SME for global DHS-component mission. Technical lead for regional integration and optimization effort to securely fuse Operational Technology input, GIS, modeling and simulation and multi-source sensors into a Common Operating Picture. Corporate director of technology and engineering for winner of Contractor of the Year 6 consecutive years; architected security and support solutions for various DoD and federal civilian agencies; senior manager responsible for overall development and operations, intrusion protection and incident handling for multiple DoD networks, spearheaded successful defense and forensic analyses of focused cyber-attacks; lead element commander for DoD's only tactical TECHINT and MASINT unit, successfully responding to more than 173 National Intelligence Requirements during eight operational deployments.

> "Mr. Williams' expertise in fusing the classic Intelligence Preparation of the Battlespace discipline with cyber operations resulted in identified and closed gaps in the enterprise RMF, increased maturity of our GRC posture, and significantly improved signal-to-noise optics and cyber situational awareness."
> **Scott S.** | *DISL* | *IC Component*

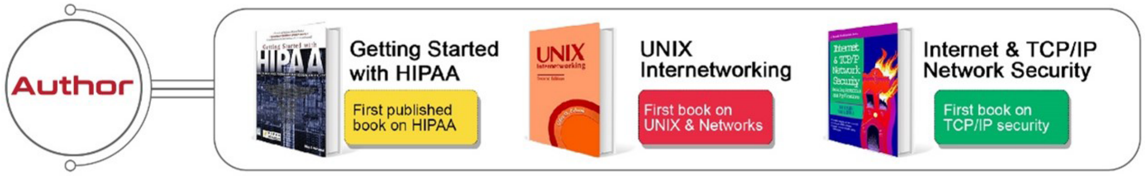
FBI Conference

"On behalf of the Idaho InfraGard (FBI), I would like to thank Pabrai for presenting at our conference. Pabrai is the kind of speaker you want to bring to executives and staff. He says it in a simple, no nonsense way, in a manner that everyone can understand."
Rachel Zahn | *President* | *InfraGard (FBI)* | *Idaho Alliance*

"You delivered a fantastic presentation and we all felt your passion for cyber security."
James E Lamadrid | *Supervisory Special Agent* | *Federal Bureau of Investigation (FBI) Cyber Task Force*

"Thank you Pabrai. Your enthusiasm and relevance for the Information Security material you presented at our combined Infragard (FBI) conference in Idaho Falls was very well received and pertinent to both our chapter as an organization and the constituents in attendance."

"As a government employee, I appreciated the simplified insight of highlighting the importance of compliance and funding compared to information security success beyond qualitative metrics. I heard many times over that your specific information with measurable results made your material directly relevant to individuals, businesses and organizations. Thanks again and I hope you are able to join us again in the future."
Clark Harshbarger | *FBI*



Author

Getting Started with HIPAA
First published book on HIPAA

UNIX Internetworking
First book on UNIX & Networks

Internet & TCP/IP Network Security
First book on TCP/IP security

HITRUST® Authorized External Assessor

r2 HITRUST CERTIFIED