CMMC

PASS YOUR UPCOMING CMMC AUDIT WITH CONFIDENCE

- Perform pre-assessment for CMMC
- Develop an SSP and POA&M
- Implement the NIST 800-171
- Pass a CMMC audit up to level 3

GET IN TOUCH

(202) 556-3903
sales@purplesec.us
purplesec.us

PURPLESEC

OFFENSIVE & DEFENSIVE CYBER SECURITY

NIST
NIST SP 800-171

CERTIFICATION

DEPARTMENT OF DEFENSE
DFARS
Compliant
UNITED STATES OF AMERICA

WHAT IS CMMC?

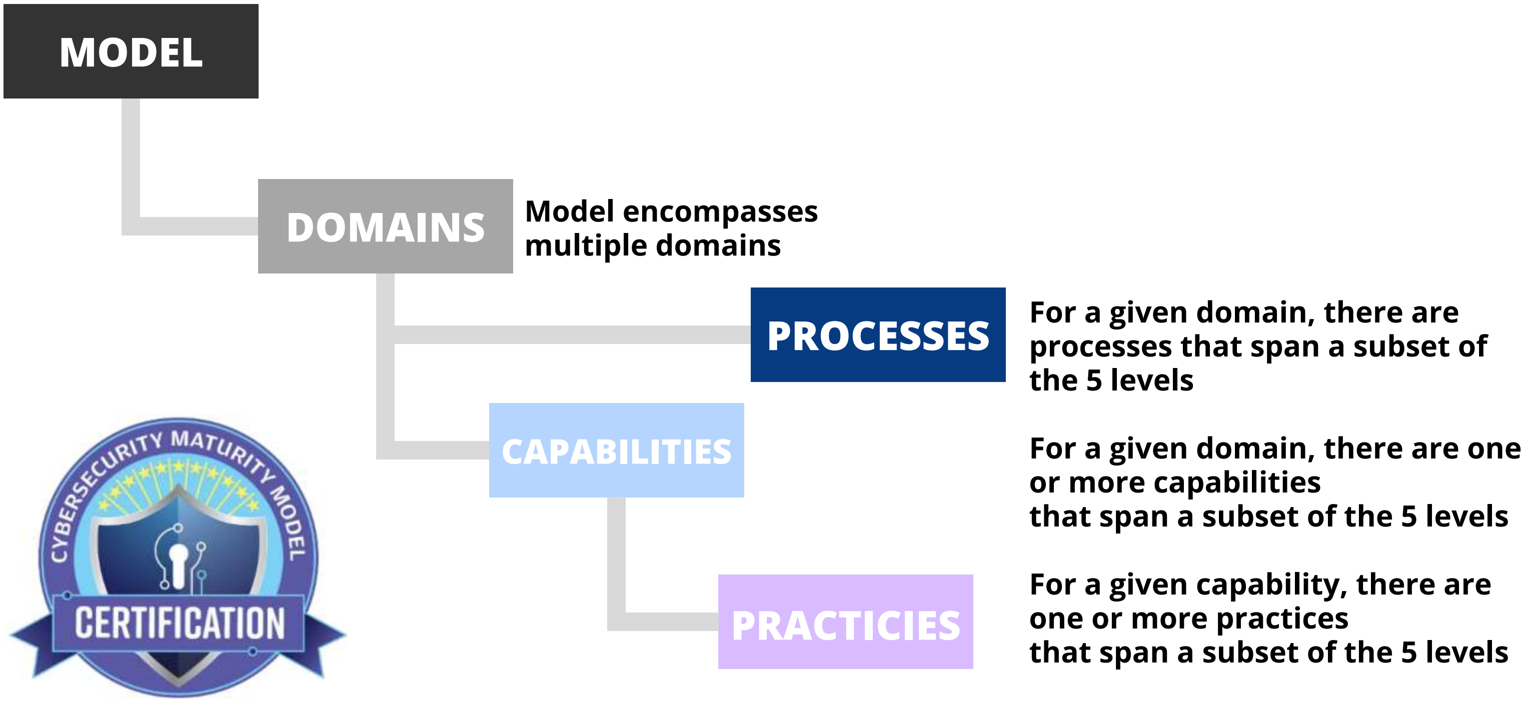
CMMC stands for the **Cybersecurity Maturity Model Certification**. The CMMC will encompass multiple maturity levels that range from Level 1: Basic Cyber Hygiene to Level 5: Advanced / Progressive.

Beginning in 2020, all contractors working for the DoD, even subcontractors must pass a CMMC Audit to ensure appropriate levels of cyber security controls and processes are adequate and in place to protect controlled unclassified information (CUI) on DoD contractor systems.

THE CMMC MODEL

In its final form, the CMMC will combine various cyber security control standards such as NIST SP 800-171 (Rev. 1 & Rev. B), NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933, DFARS 252.204-7012, FAR 52.204-21, and others into one unified standard for cyber security.

The intent is to identify the required CMMC level for Department of Defense Contractors in RFP sections as a "go / no go decision."



MODEL

DOMAINS **Model encompasses multiple domains**

PROCESSES **For a given domain, there are processes that span a subset of the 5 levels**

CAPABILITIES **For a given domain, there are one or more capabilities that span a subset of the 5 levels**

PRACTICIES **For a given capability, there are one or more practices that span a subset of the 5 levels**

HOW CAN YOU PREPARE?

STEP 1

Step one is to get NIST 800-171 documentation out of the way.

You can do a self-assessment of the 800-171 controls or hire a third-party service company to do a GAP analysis to determine your current level of compliance.

Auditors will do a by the book assessment against the current CMMC version and create a roadmap to compliance toward the final 1.0 version.

This is your opportunity to get 90% of the work done before the competition and ahead of the last-minute rush to get validated.

STEP 2

The second step is to map your 800-171 assessment to the CMMC requirements once they're released.

Be ready to address the gaps you find during mapping and implement solutions to remediate them. CMMC audits can help provide you with an SSP, POAM and remediation actions to complete.

STEP 3

The third step is to find an authorized 3rd party to audit your assessment and give you a certification for the level you need.

You should have no trouble finding an auditor even before the requirements are released since it's very likely existing 800-171 service companies will transition to CMMC auditors.

CMMC LEVELS

LEVEL 1

BASIC CYBER HYGIENE

17 PRACTICES

- Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2

INTERMEDIATE CYBER HYGIENE

72 PRACTICES

- Comply with FAR
- Includes a select subset of 48 practices from NIST SP 800-171 r1
- Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3

INTERMEDIATE CYBER HYGIENE

130 PRACTICES

- Comply with FAR
- Encompasses all practices from NIST SP 800-171 r1
- Includes an additional 20 practices to support good cyber hygiene.

LEVEL 4

PROACTIVE

156 PRACTICES

- Comply with FAR
- Encompasses all practices from NIST SP 800-171 r1
- Includes a select subset of 11 practices from Draft NIST SP 800-171B
- Includes an additional 15 practices to demonstrate a proactive cybersecurity program.

LEVEL 5

ADVANCED/PROGRESSIVE

171 PRACTICES

- Comply with FAR
- Encompasses all practices from NIST SP 800-171 r1
- Includes a select subset of 4 practices from Draft NIST SP 800-171B
- Includes an additional 11 practices to demonstrate an advanced cybersecurity program.

17 CAPABILITY DOMAINS

V1.0

Access Controls	Incident Response	Risk Management	Assess Management
Maintenance	Security Assessment	Awareness Training	Media Protection
Situational Awareness	Audit & Accountability	Personal Security	System Coms. Protection
Configuration Management	Physical Protection	System & Info. Integrity	
Identification & Authentication	Recovery		

CMMC & NIST 800-171

Many of the same controls that are in the National Institute of Standards and Technology (NIST) 800-171 will be included in CMMC along with controls from other standards such as ISO, FedRAMP, and various NIST frameworks.

CMMC also requires a 3rd party audit in order to gain certification, whereas 800-171 is a “self-certification”.

Existing DoD contracts that contain the 252.204-7012 DFARS clause will still require your organization to provide documentation proving compliance with NIST 800-171.

We don’t know if Contracting Officers will be asked to modify active contracts to swap CMMC and 800-171.

This may end up being a per-contract decision. CMMC is different than NIST 800-171, but the controls can be mapped from 800-171 to the levels of certification within CMMC.

CMMC LEVEL	TOTAL NUMBER PRACTICES	SOURCE			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B**	Other
LEVEL 1	17	15*	17*	-	-
LEVEL 2	55	-	48	-	7
LEVEL 3	58	-	45	-	13
LEVEL 4	26	-	-	11	15
LEVEL 5	15	-	-	4	11

*** Note: 15 safeguarding requirements from FAR clause 52.204-21 correspond to 17 security requirements from NIST SP 800-171r1, and in turn, 17 practices in CMMC**

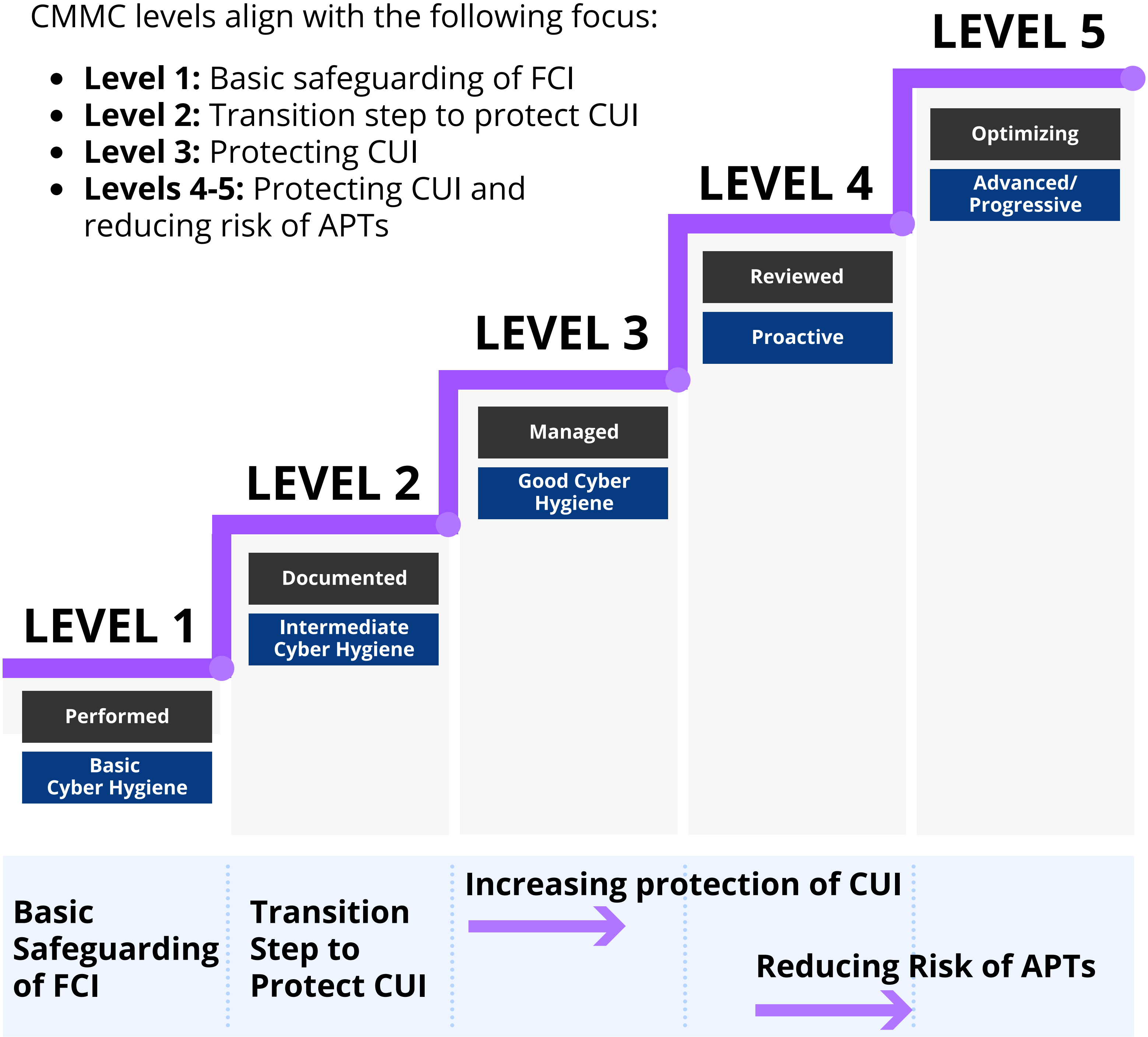
**** Note: 18 enhanced security requirements from Draft NIST SP 800-171B have been excluded from CMMC Model v1.0**

SUMMARY

CMMC establishes cyber security as a foundation for future DoD acquisitions.

CMMC levels align with the following focus:

- **Level 1:** Basic safeguarding of FCI
- **Level 2:** Transition step to protect CUI
- **Level 3:** Protecting CUI
- **Levels 4-5:** Protecting CUI and reducing risk of APTs



LEVEL 1

Performed

Basic Cyber Hygiene

LEVEL 2

Documented

Intermediate Cyber Hygiene

LEVEL 3

Managed

Good Cyber Hygiene

LEVEL 4

Reviewed

Proactive

LEVEL 5

Optimizing

Advanced/ Progressive

Basic Safeguarding of FCI

Transition Step to Protect CUI

Increasing protection of CUI →

Reducing Risk of APTs →

CMMC FAQS

When Will The CMMC Framework Be Available To The Public?

The DoD released version 1.2 in March 2020. This leaves contractors with less than 3 months to prepare before CMMC starts appearing in Requests for Information (RFIs) in 2021.

What If We Do Not Handle CUI? Will We Need To Be Certified?

Yes. All companies doing business with the Department of Defense will need to obtain CMMC Even if you are a subcontractor.

How Often Do I Need To Be Recertified?

We're not sure yet. They are still considering that part. The CMMC Accreditation Body will make that determination.

Who Will Be Accrediting CMMC Auditors?

The Office of the Undersecretary of Defense (Acquisition & Sustainment) (OUSD(A&S)) in the Department of Defense has issued an RFI (Request for Information), to determine if a non-profit entity could successfully function as the Accreditation Body for CMMC.

REACH 100% COMPLIANCE MONTHS BEFORE THE AUDIT COMES

✓ **CONDUCT A CMMC GAP ANALYSIS**

✓ **IMPLMENT THE NIST 800-171 FRAMEWORK**

✓ **POAM&M AND SSP ASSISTANCE**

✓ **PASS AN UPCOMING CMMC AUDIT UP TO LEVEL 3**

GET A FREE CONSULTATION

PURPLESEC