

# CMMC L2 Certification Assessment

## Common Pitfalls



by KLC Consulting, Inc.  
*Authorized C3PAO Company*

April 2025



\* Some contents in this presentation are from the DoD CMMC Briefing

All Rights Reserved



# About KLC Consulting



- We're a CMMC 3<sup>rd</sup> Party Assessment Organization (C3PAO), authorized by the DoD and CyberAB to assess and certify companies in CMMC.
- KLC Consulting is also a CMMC Compliance Consulting firm that helps DIB companies meet the U.S. DoD information security requirements.
- We were incorporated in 2002. We have offices in Boston, Massachusetts and Houston, Texas.



# Presenter



## Kyle Lai

**President and CISO**  
**KLC Consulting**

Lead CMMC Certified Assessor (LCCA)  
CISSP, CSSLP, CISA, CDPSE, CIPP/US/G,

Email: [Klai@klcconsulting.net](mailto:Klai@klcconsulting.net)

LinkedIn: <https://www.linkedin.com/in/kylelai>



- Former DISA (DoD) Operations Manager
- Former CISO of a Blackstone Subsidiary & Brandeis University – Heller School
- Former Penetration Tester for Fortune 500 firms
- Author of SMAC MAC Address Changer – Over 3 million users
- 25+ years in IT and 20 years in Cybersecurity (Pentest, Third-party Risk, Compliance, Privacy, Engineering...)

- Security Advisor to Fortune 500 companies
- Experience with Software, DoD, Financial, Energy, Healthcare, High Tech, and Consulting industries
- Security advisory for Microsoft, Boeing, Fidelity Investment, Akamai, ExxonMobil, DISA, Zoom
- SME on CMMC, NIST 800-171, NIST 800-53, DoD RMF
- Creator of the SMAC MAC Address Changer (SMAC) tool

# Email Us Your Feedback, Questions, & CMMC Journey

Email to: [cmmc-feedback@KLCConsulting.net](mailto:cmmc-feedback@KLCConsulting.net)

We will send you today's presentation.



**We welcome your feedback:**

1. Where are you on your CMMC Journey?
2. What is the most challenging part of the CMMC Compliance?
3. Your feedback on our presentation is welcome.



# CMMC-PNW

# Conference

## Agenda

- ❖ CMMC Overview
- ❖ CMMC Level 2 Certification Assessment Process
- ❖ Common Pitfalls
- ❖ Q&A





# Acronyms

C3PAO	CMMC Third-Party Assessment Organization	MSSP	Managed Security Service Provider
CAICO	CMMC Assessors and Instructors Certification Organization	NARA	National Archives and Records Administration
CAGE	Commercial and Government Entity	NAICS	North American Industry Classification System
CCA	CMMC Certified Assessor	NIST	National Institute of Standards and Technology
CCP	CMMC Certified Professional	N/A	Not Applicable
CFR	Code of Federal Regulations	ODP	Organization-Defined Parameter
CMMC	Cybersecurity Maturity Model Certification	OSA	Organization Seeking Assessment
CMMC PMO	CMMC Program Management Office	OSC	Organization Seeking Certification
CUI	Controlled Unclassified Information	OT	Operational Technology
DFARS	Defense Federal Acquisition Regulation Supplement	PIEE	Procurement Integrated Enterprise Environment
DIB	Defense Industrial Base	PLC	Programmable Logic Controller
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center	POA&M	Plan of Action and Milestones
DoD	Department of Defense	PRA	Paperwork Reduction Act
eMASS	Enterprise Mission Assurance Support Service	RM	Risk Management
ESP	External Service Provider	SAM	System for Award Management
FAR	Federal Acquisition Regulation	SCADA	Supervisory Control and Data Acquisition
FCI	Federal Contract Information	SIEM	Security Information and Event Management
FedRAMP	Federal Risk and Authorization Management Program	SP	Special Publication
IoT	Internet of Things	SPRS	Supplier Performance Risk System
IR	Incident Response	SSP	System Security Plan
MSP	Managed Service Provider		



# CMMC Levels

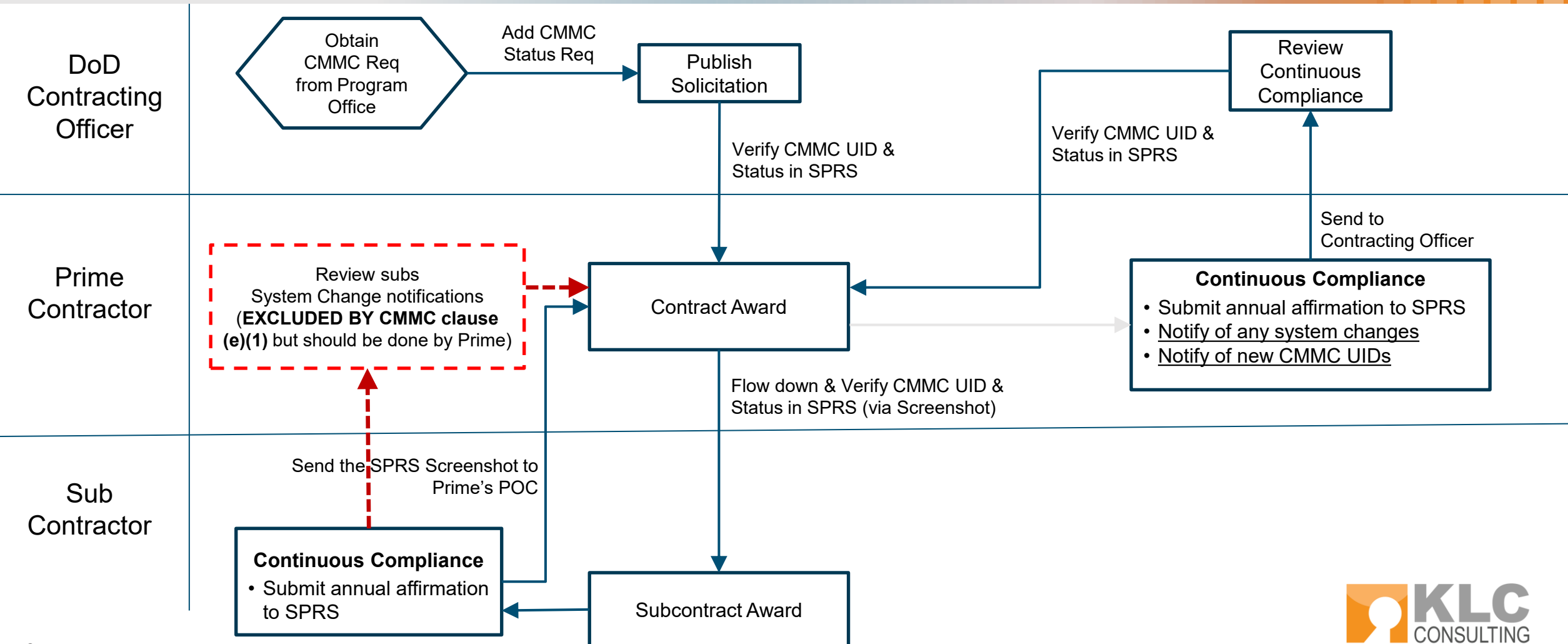
CMMC Model	
Model	Assessment
<b>LEVEL 3</b> 134 Requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	<ul style="list-style-type: none"><li>• DIBCAC assessment every 3 years</li><li>• Annual Affirmation</li></ul>
<b>LEVEL 2</b> 110 Requirements aligned with NIST SP 800-171 r2	<ul style="list-style-type: none"><li>• C3PAO assessment every 3 yrs., or</li><li>• Self-assessment every 3 years for select programs</li><li>• Annual Affirmation</li></ul>
<b>LEVEL 1</b> 15 Requirements aligned with FAR 52.204-21	<ul style="list-style-type: none"><li>• Annual self-assessment</li><li>• Annual affirmation</li></ul>

## 3 Progressive Levels

- **Level 1** – Basic Safeguarding of FCI  
Based on FAR 52.204-21  
(6 Domains, 15 requirements)
- **Level 2** – Broad Protection of CUI  
Based on NIST 800-171 **Rev 2**  
(14 Domains, 110 requirements)
- **Level 3** – Higher-Level Protection of CUI against APT. Based on NIST 800-171 **Rev 2** and 800-172 (110 requirements + 24 additional objectives)

# CMMC Final Rule – Simple View

## DFARS 252.204-7021





# CMMC Implementation Timeline

## Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

11/10/2025

**In some procurements, DoD may implement CMMC requirements in advance of the planned phase**

## Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

11/10/2026

## Phase 3

- Begins 24 months after Phase 1 start
- Where applicable, solicitations will require Level 3 Certification

11/10/2027

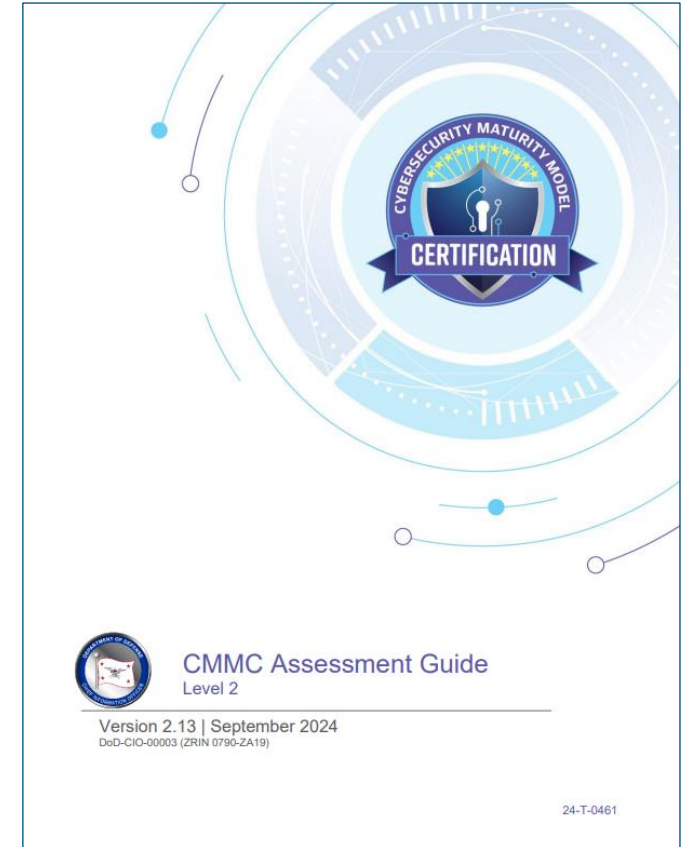
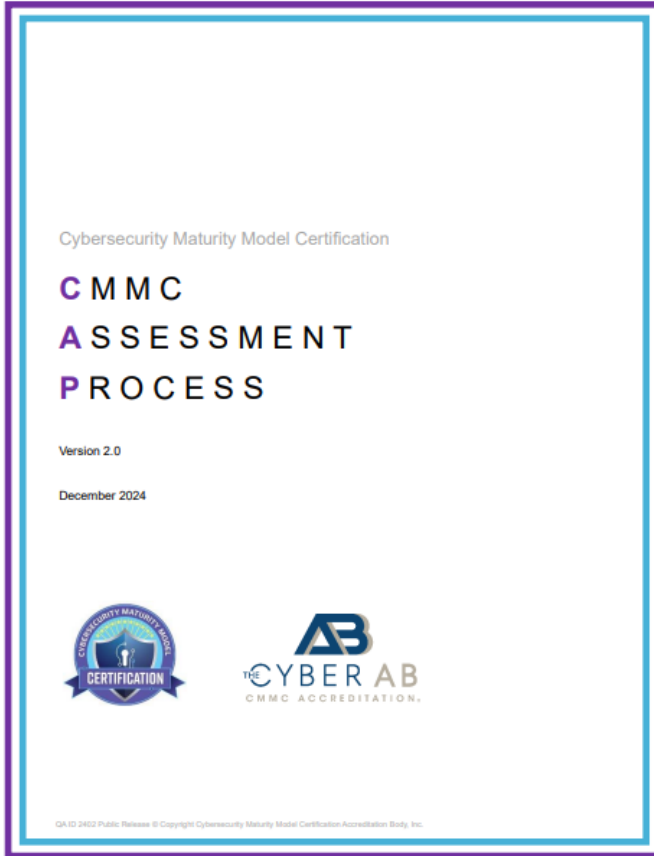
## Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

11/10/2028



# Important CMMC Resource Documents



Download from [CyberAB](#) and [DoD CMMC Program Website](#):

# Typical CMMC Level 2 Certification Assessment



## Assessment Planning

- ✓ Provide assessment schedule and scoping agenda
- ✓ Hold Assessment Phase Kickoff Meeting (scope, diagrams, SSP overview)
- ✓ OSC uploads the supporting artifacts to the agreed file-sharing platform
- ✓ Formalize and finalize Assessment Plan

## Assessment Interview Week

- C3PAO Conducts daily assessments and interviews
- ✓ Day 1: C3PAO provides Assessment In-Brief
  - ✓ C3PAO provides Daily touchpoints and progress updates (hotwash)
  - ✓ C3PAO conducts on-site physical inspection (if applicable)
  - ✓ Last Day: C3PAO provides Preliminary Findings (MET vs. NOT MET)

## 10 Business Days After Assessment

- ✓ Day OSC provides additional evidence for NOT-MET items if needed

## Post Assessment

- ✓ C3PAO provides final assessment out-brief and results summary
- ✓ Results uploaded into eMASS; Certificate (Conditional or Final) issued
- ✓ eMASS updates the certificate status to the SPRS

## CMMC Level 2 Assessment Process

- Preparing for Your CMMC Assessment: [A Guide for OSCs](#)
- Follows the CyberAB CMMC Assessment Process (CAP)

# What Do Assessors Look For?

## Download Our Free Playbook

Get clear insights into C3PAO expectations for each security requirement and what evidence they'll require. Be fully prepared to ace your assessment.

<https://klcconsulting.net/cmmc-resource-tools/>





# Objective Evidence Checklist

OBJECTIVE	SECURITY REQUIREMENT	TEAM INPUT	EVIDENCE EXAMPLES (ASSESSORS ARE NOT LIMITED OR RESTRICTED TO EXAMPLES)	CMMC ASSESSMENT CONSIDERATIONS (CMMC Assessment Guide - Level 2)
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			
3.1.1[a]	Authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	Is a list of authorized users maintained that defines their identities and roles?
3.1.1[b]	Processes acting on behalf of authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[c]	Devices (and other systems) authorized to connect to the system are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[d]	System access is limited to authorized users.	Screen Share	Screen share showing login requirements are enforced. Example of an unauthorized user denied (Unauthorized username entered at login)	Are account requests authorized before system access is granted?
3.1.1[e]	System access is limited to processes acting on behalf of authorized users.	Screen Share	Screen shot showing that service accounts are assigned to authorized users only. No rogue accounts without an authorized user are active.	Are account requests authorized before system access is granted?
3.1.1[f]	System access is limited to authorized devices (including other systems).	Screen Share	Screen share showing that all devices running are authorized. No rogue devices on the network.	Are account requests authorized before system access is granted?
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.			
3.1.2[a]	The types of transactions and functions that authorized users are permitted to execute are defined.	Document	SSP, AUP, or IAM document that defines what authorized users can execute.	Are access control lists used to limit access to applications and data based on role and/or identity?
3.1.2[b]	System access is limited to the defined types of transactions and functions for authorized users.	Screen Share	Screen shot of security roles in AD or IAM tool that shows transactions are as defined in the SSP or IAM document. Privileged and Non-privileged accounts need to be defined and identified in the artifact. Screenshot of a non-privileged user trying to execute a privileged function.	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)?

# CMMC L2 Assessment Common Mistakes



1

## Inadequate Artifacts and Demo Preparation

- OSCs are unclear about which artifacts to present for each requirement and during the on-site physical inspection.

2

## Existing Practices Do Not Match the Documented Processes

- Security tasks (e.g., log review, vulnerability scans, patch management) are not performed as described in the SSP.

3

## No Mock Assessment (Practice Test) Before the Official Certification Assessment

- CMMC documentation was not reviewed by a CMMC SME for adequacy or sufficiency.

# CMMC L2 Assessment Common Mistakes



4

**CMMC Scope, Boundary, and Asset Inventory are Not Adequately Updated**

- SSP does not reflect the actual in-scope systems and devices, as well as the internal and external connections.

5

**Configuration Baselines Not Sufficiently Documented**

- Configuration Baselines must be documented for each type of asset (e.g., Windows laptops, Linux servers, Firewall).

6

**Undocumented Specialized Assets (SA) and Contractor Risk Managed Assets (CRMA)**

- SAs and CRMAs are not in the boundary, scope, asset inventory, and SSP.
- SA and CRMAs must be documented in the SSP – but not be tested for CMMC Level 2.

# CMMC L2 Assessment Common Mistakes



7

**Misunderstood Operational Plan of Action (OPoA) vs Plan of Action & Milestone (POA&M)**

- Lack of understanding of OPoA (CMMC specific term) vs POA&M.
- OPoA items = MET. POA&M items = NOT MET.

8

**Unclear ESP (CSP/MSP) Inheritance and Shared Responsibility Documentation**

- For each requirement, a lack of indication of fully or partially inherited controls from CSP/MSP.

9

**Missing ESP (CSP/MSP) Evidence**

- FedRAMP documentation (e.g., Body of Evidence and Customer Responsibility Matrix) not provided as CSP artifacts.
- Lack of documentation and evidence on the MSP's responsibilities and processes (e.g., firewall management)

# CMMC L2 Assessment Common Mistakes



10

## Key Personnel or MSP Staff Not Present During the Assessment

- Key personnel are unavailable during the assessment, resulting in delays and unanswered questions.

11

## Missing Software / Software Development Systems in the Scope

- Custom-developed software that stores, transmits, or processes CUI is not included in the boundary diagram, scope diagram, asset inventory, and SSP.  
(**Note:** Source code may be CUI).



# CMMC – Tips for Success

## Proper Scoping Via CMMC Scoping Guide

- Define CUI Asset (People, Facilities, Tools)
- Security Protection Asset
- Contractor Risk Managed Asset
- Specialized Asset
- Out-of-Scope Asset

## Accurate Gap Assessment

- By experts in CMMC
- Document and prioritize gaps
- Budget for remediation
- This isn't the place for DIY!

## Dedicated Resources Senior Management Support

- Support from Sr. Management
- Dedicated project manager
- Support from IT staff
- Staff training for people handling CUI
- Get outside expert help if no internal CMMC-certified SME!

# Thank You!



CMMC / AUTHORIZED C3PAO

[www.klcconsulting.net](http://www.klcconsulting.net)

## Get in Touch with Us!



617.314.9721. x168



[cmmc@klcconsulting.net](mailto:cmmc@klcconsulting.net)



<https://www.linkedin.com/in/kylelai/>



[KLC Consulting YouTube Channel](#)

