# CMMC – What Contractors Need to Know Now

**SAME Space Coast | April 16, 2026**

Presenter:
Elizabeth Huy, EVP Commercial Services

# Agenda

- Introduction
- CMMC Final Rule
- Primes vs Subs: Reality Check
- CMMC Ecosystem – By the Numbers
- Compliance Process
- CMMC Domains and Your Team
- Choosing the Right Partners
- Cost Considerations
- Lessons Learned

# Introduction

## Elizabeth Huy

EVP, Commercial Services

PMP® | Cyber-AB RP

ehuy@alluvionic.com | alluvionic.com

### About me

- Leads Commercial Business Unit at Alluvionic – Cybersecurity, Project Management and Process Improvement Services.
- Owns strategy, business development, budgeting, resourcing, and execution
- Accountable for scaling delivery and ensuring successful client outcomes
- Education: B.S. in Finance and Marketing, Florida State University
- Outside of work: wife, mom of two teenage boys, dog + cat, distance runner (for fun), BOD for EDC, Space Coast Chamber and Chair of the City of Melbourne's Historic & Architectural Review Board (HARB)

Alluvionic® PROJECT ASSURANCE®

**Cyber AB - RPO**
Since 2020

**CMMC L2**
Certified

**180+**
CMMC Clients Served

### About Alluvionic

- One of the first Cyber-AB Registered Practitioner Organizations (since 2020)
- We've achieved CMMC Level 2 ourselves — not just advised on it
- Support across the full lifecycle: strategy → implementation → assessment readiness
- Credentialed, experienced professionals – CCP, PMP, CISSP, CISA, CISA +

**CERTIFICATIONS & PARTNERSHIPS**

CMMC Level 2 | Cyber-AB Registered Practitioner Organization | ISO 9001:2015 | CMMI Institute Partner | PMI Authorized Training Partner | Smartsheet Aligned Partner

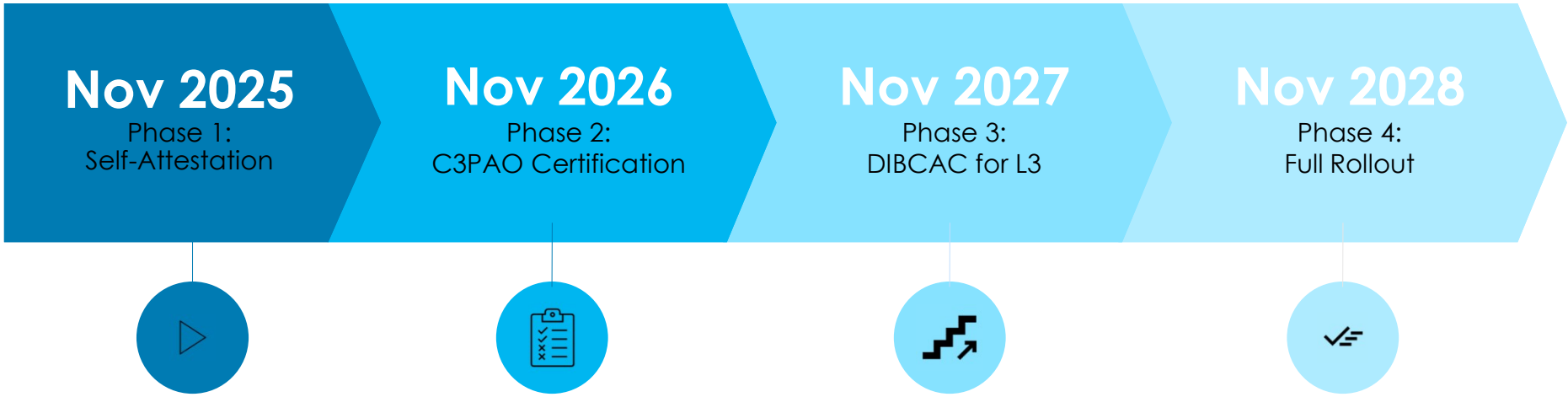
**We don't just advise on CMMC — we help you implement, operationalize, and pass.**


© Alluvionic

# CMMC – What Contractors Need to Know Now

# DFARS 252.204-7021 – Final, Effective…And in a Contract Near You

***It's no longer theoretical — CMMC is in contracts now.***




SPRS Attestation for CMMC L1 or L2 100% Compliance Expected

Authorized to start requiring 3rd Party Certification for L2 – won't hit all at once

High Sensitivity Contracts will require L3 (less than 1% of DIB). Most contracts will now require 3rd party validation

All Contracts will include CMMC Requirements (COTS excluded)

# Reality Check: Primes Are Moving Faster Than the DoD

April 6, 2026

**SUBJECT: CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) – Action Needed**

Supplier Team Members.

[redacted] has been closely monitoring the DoD's development of the new Cybersecurity Maturity Model Certification (CMMC) process. The purpose of this letter is to ensure all suppliers on DoD programs are aware of and preparing for CMMC.

CMMC 48 CFR is the final rule making CMMC enforceable in DoD contracts, published in the Federal Register on September 10, 2025, with an effective date of November 10, 2025. This marks the official start of Phase 1 of the CMMC rollout, meaning readiness is mandatory for all new DoD solicitations and contracts, which now include some level of CMMC requirement. There are three levels of certification (from 1 to 3), with Level 2 being the minimum for processing Controlled Unclassified Information (CUI). CMMC compliance is required in order to be awarded a contract. If you haven't started your CMMC certification process, contacting a C3PAO (CMMC Third Party Assessment Organization) should be a priority.

All suppliers on DoD programs who receive CUI at all tiers must be certified if required by the DoD prime contract, including small businesses and foreign suppliers. Certification may be needed to submit a proposal and prior to the contract award. Suppliers who do not qualify for certification at Level 2 will be precluded from the program. This requirement does not apply to suppliers who solely produce commercial-off-the-shelf (COTS) items as defined in FAR 2.101..

To maintain compliance and the integrity of our supply chain, [redacted] requires all suppliers to provide documentation verifying their CMMC Level 2 certification. This includes:

- A copy of your CMMC Level 2 assessment report.
- A copy of your CMMC Level 2 certificate issued by a C3PAO.

These documents are essential for us to verify that our suppliers adhere to the necessary cybersecurity standards mandated by our contract awards. As we are starting to see contracts from our customers with these requirements, we are requesting that our suppliers become certified **no later than July 30, 2026**. We request you submit the required documentation at your earliest convenience to ensure there are no disruptions to our business operations. Please send the requested documents to [redacted]

We appreciate your prompt attention to this critical requirement and look forward to continuing our successful business relationship. Thank you for your cooperation.

## What This Means for Subs

### Prime Requirements Exceed DoD Minimums

Example Prime letter sent April 6, 2026 requiring all suppliers to achieve CMMC Level 2 by July 30, 2026 — months before DoD Phase 2.

### What They're Expecting

A copy of your Level 2 assessment report and your CMMC certificate issued by a C3PAO. Non-compliance risks your spot on the program.

### Flow-Downs Are Contractual… and Primes are Risk Averse

Prime flow-down requirements are legally enforceable via your subcontract. 'COTS suppliers only' are exempt; everyone else is on the hook.

### The Clock Is Already Running

If a prime has already sent you a letter — or will soon — you may have less time than the government's November 2026 deadline suggests.

# The CMMC Ecosystem – By the Numbers

**~80,000**

DoD contractors expected to require CMMC Level 2

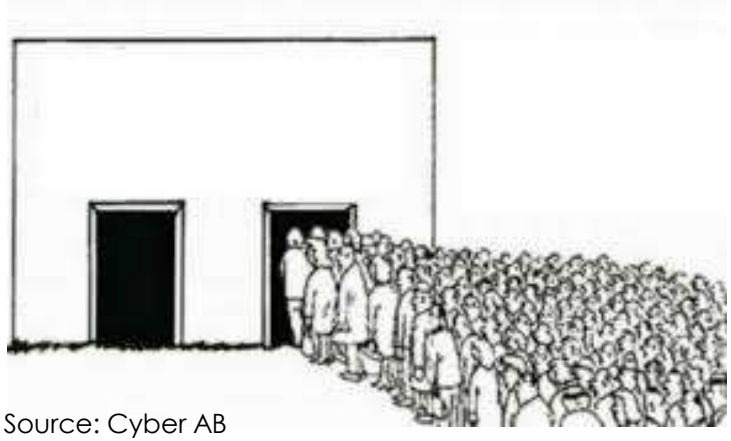
**1,074**

Certificates of CMMC Status FINAL (March 2026)

**39**

Conditional certificates (6 months to remediate)

🏃 Waiting = longer queues, higher cost, schedule risk



Source: Cyber AB

## What This Means

📊 Only ~1% certified — ~79,000 still in line

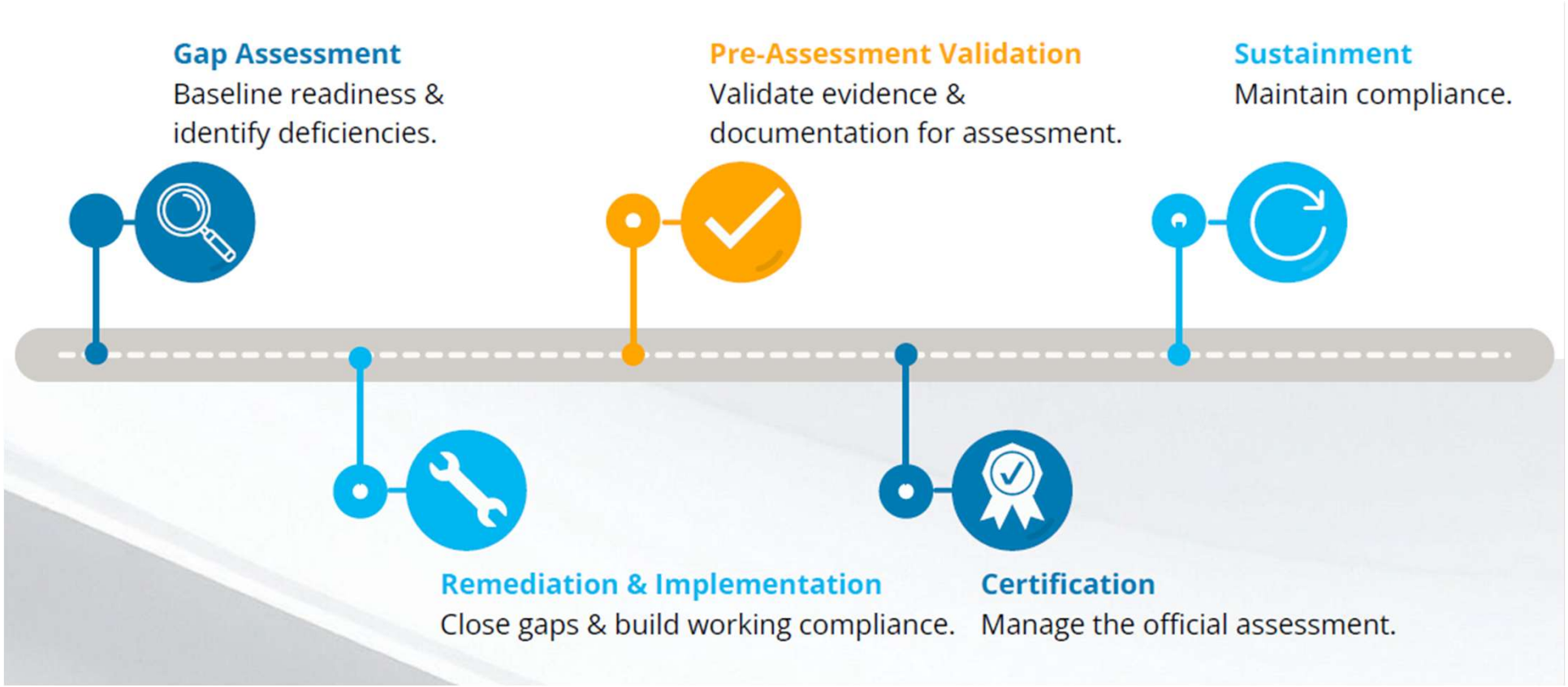
🏛️ Only 103 authorized C3PAOs to assess them all

⏳ Demand massively exceeds assessor capacity

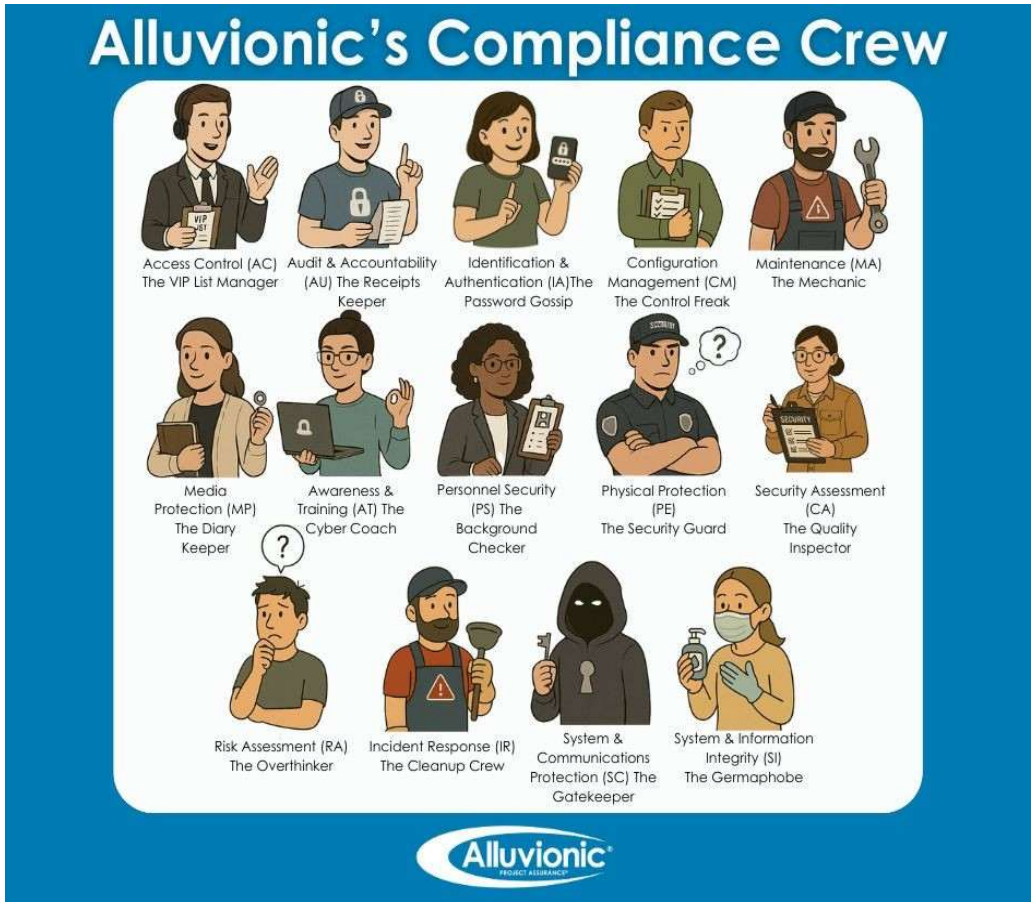
🔄 Many assessments start & get kicked back before completion - false starts not counted in these numbers

📈 GAO report (2025): critical concerns about ecosystem capacity and readiness

# CMMC Compliance Process



# What Does CMMC Cover + Who Should be Involved?




## 14 Domains, 110 Controls, 320 Objectives

CMMC Level 2 maps to NIST SP 800-171 rev2 and it touches every part of your organization.

- Access Control (AC)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System & Comms Protection (SC)
- System & Info Integrity (SI)
- Awareness & Training (AT)

**⚠ This is NOT just an IT problem — it requires HR, legal, facilities, operations, marketing and executive leadership.**

# Buyer's Guide: How to Find the Right Partners

*Different partners serve different roles — success comes from aligning strategy, implementation, and assessment.*

## RPOs & Consultants

*Strategy + Readiness*

- Proven CMMC/NIST 800-171 expertise — look for CCP credentials
- Experience with your industry & environment type
- Structured readiness approach: gap assessment → POA&M → SSP
- Clear methodology for scoping CUI and reducing assessment scope
- OCM Focus - practical implementation, not just documentation
- Experience through C3PAO Assessments and guides your team on what to expect
- Strong alignment with current C3PAO expectations & trends

## IT MSPs

*Tech Implementation + Ongoing Support*

- Demonstrated CMMC experience with active, compliant clients
- Alignment with NIST 800-171: SRM, policies, and evidence support
- Secure architecture: MFA, encryption, network segmentation, FedRamp
- Ongoing vulnerability management, patching & risk remediation
- 24/7 monitoring, SIEM, and incident response capability
- Backup, recovery, and FedRAMP-aligned cloud practices
- Clear shared responsibility model + transparent pricing

## C3PAOs

*Assessment + Certification*

- How many assessments have they completed & outcomes? Ask directly.
- Current backlog and realistic scheduling timelines
- Experience with your sector, size, and system complexity
- Clear, transparent assessment process and expectations
- Defined evidence requirements and level of rigor
- Ability to perform virtual vs. on-site assessments
- Independence from your consultant — no conflicts of interest

# How Much is this going to cost?

## 💰 Cost: The Honest Answer — "It Depends"

*From our Small Business CMMC Survey — costs vary significantly:*

**Scope of your CUI environment**
Smaller boundary = lower cost and faster implementation + assessment

**Number of systems & users**
Each adds time and complexity

**Readiness level at start**
Gaps found during assessment = cost overruns

**Internal resource availability**
Your team's time and responsiveness matters


*Source: Alluvionic Small Business Survey*

**Key Message**

The cheapest option upfront is often the most expensive long-term. A false start — going through assessment before you're ready — means restarting the clock, paying twice, and potentially missing contract deadlines.

# Lessons Learned: A Tale of Two Approaches

*Real patterns we see — names changed, stories are true*

## ❌ The False Start

✗ **Only IT lead involved:**

No executive sponsor engagement, no cross-functional team

✗ **Minimal external expertise:**

Strong resistance to investment in tools or outside support

✗ **Poor scoping:**

Systems and users missed — CUI boundary was incomplete

✗ **Started too early:**

Assessment kicked back — gaps not remediated before assessment began

✗ **Result:**

Restarted from scratch. Paid ~2x in time, money, and disruption. Delivery schedule impacted.

## ✅ The Right Approach

✓ **Executive sponsor identified:**

Leadership owned CMMC from day one — not just IT

✓ **Cross-functional team:**

HR, operations, IT, and legal all at the table

✓ **RPO engaged early:**

Gap analysis done first; remediation plan built, implementation completed before assessment

✓ **Formal scoping & SSP:**

CUI boundary documented; System Security Plan completed. Documentation tested; Team trained.

✓ **Result:**

Passed first assessment. On schedule. Within budget. Zero surprises.

# Key Takeaways — What To Do Next

**1** **Start earlier than you think**

Assessor backlog is real. C3PAO queues are growing. Every week of delay adds risk.

**2** **Involve more than IT**

CMMC is an organizational effort. Executive leadership is critical — not just buy-in.

**3** **Self-attestation is a legal commitment**

You are certifying 100% compliance. Partial compliance is not an option.

**4** **Watch your prime flow-downs**

Your deadline may already be earlier than November 2026. Read your subcontracts.

**5** **Validate your partners**

Look for CCPs + CCAs on staff, C3PAO experience, and ask if they've done it themselves.

**Free Webinar**
**CMMC False Starts**

**Tuesday, April 28, 2026**
**12:00–1:00 PM ET**
**1 PMI PDU**

Register:
alluvionic.com/events

**Questions? Contact Alluvionic:**

ehuy@alluvionic.com | alluvionic.com | Melbourne, FL

# Questions and Answers

Alluvionic®
PROJECT ASSURANCE®

# Thank You!