ISI

STEAL OUR CMMC LEVEL 2 READINESS STRATEGY

A Practical Guide to Achieving CMMC Compliance

WE'VE BEEN THROUGH IT— NOW WE'RE SHARING WHAT WORKS

ISI successfully completed our **CMMC Level 2 assessment**, giving us firsthand insight into what it takes to **prepare, pass, and maintain compliance**. This deck provides:

A PROVEN ROADMAP

Step-by-step guidance to navigate CMMC Compliance

HOW TO PREPARE

Key actions before your assessment to avoid setbacks

REMEDIATION INSIGHTS

Addressing gaps and strengthening security

FINAL STEPS FOR SUCCESS

What to expect before, during, and after your assessment

OUR FIRSTHAND TAKEAWAYS

Jump ahead to slide 11 for our key takeaways

UNDERSTANDING THE CMMC TIMELINE

STEP 1

GET YOUR HOUSE IN ORDER

1. Identify Your CMMC Level
2. Specify Your CMMC Assets
3. Adopt a Technical Approach
4. Ensure Cloud Compliance
5. Plan, Record, Adopt

STEP 2

CMMC CERTIFICATIONS AVAILABLE

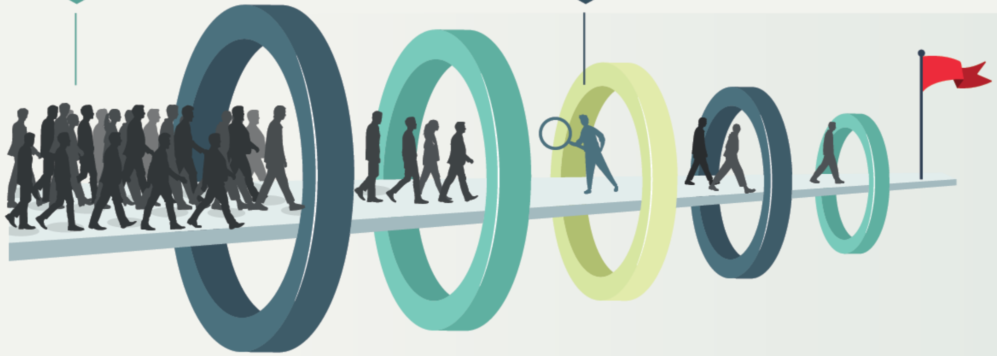
CMMC assessments are available. However, there are currently ~65 C3PAO assessors.

STEP 3

CMMC ROLLOUT BEGINS!

The CMMC rollout will start in **Q2 of 2025**, and the requirement will begin to be included in select DoD contracts.

Join the line.



70,000+ DoD Contractors

~65 C3PAO Assessors

Now that you've obtained your CMMC level 2 certificate, you have:

- Enhanced security posture
- Remained eligible for DoD contracts
- Solidified business reputation and trust

CMMC is here. Contractors who want to protect existing contracts and stay competitive for future opportunities must act now.

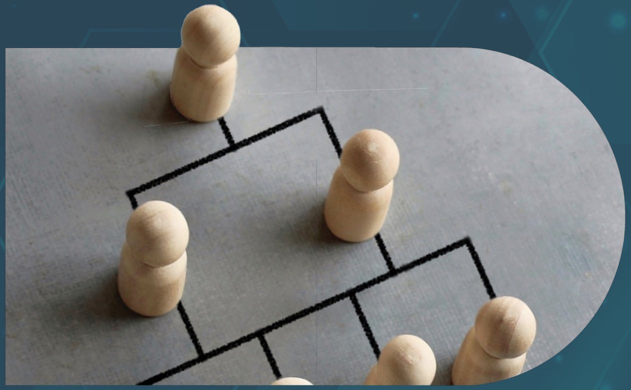
Compliance isn't just a requirement—it's a strategic advantage.

ARE YOU IN SCOPE FOR CMMC LEVEL 2?

You’re required to achieve **CMMC Level 2** if:

1 Your contracts contain **DFARS 7012** language

2 You handle **controlled unclassified information (CUI)** for DoD contracts



3 A prime contractor requires it for subcontracting eligibility

WHY IT MATTERS: Non-compliance means lost contracts and limited business opportunities in the defense sector.

THREE WAYS YOU'LL BE ASSESSED

CMMC Level 2 is based on NIST 800-171, requiring the implementation of 110 security controls mapped across 320 assessment objectives.

EXAMINE

Review of policies, procedures, and documentation

INTERVIEW

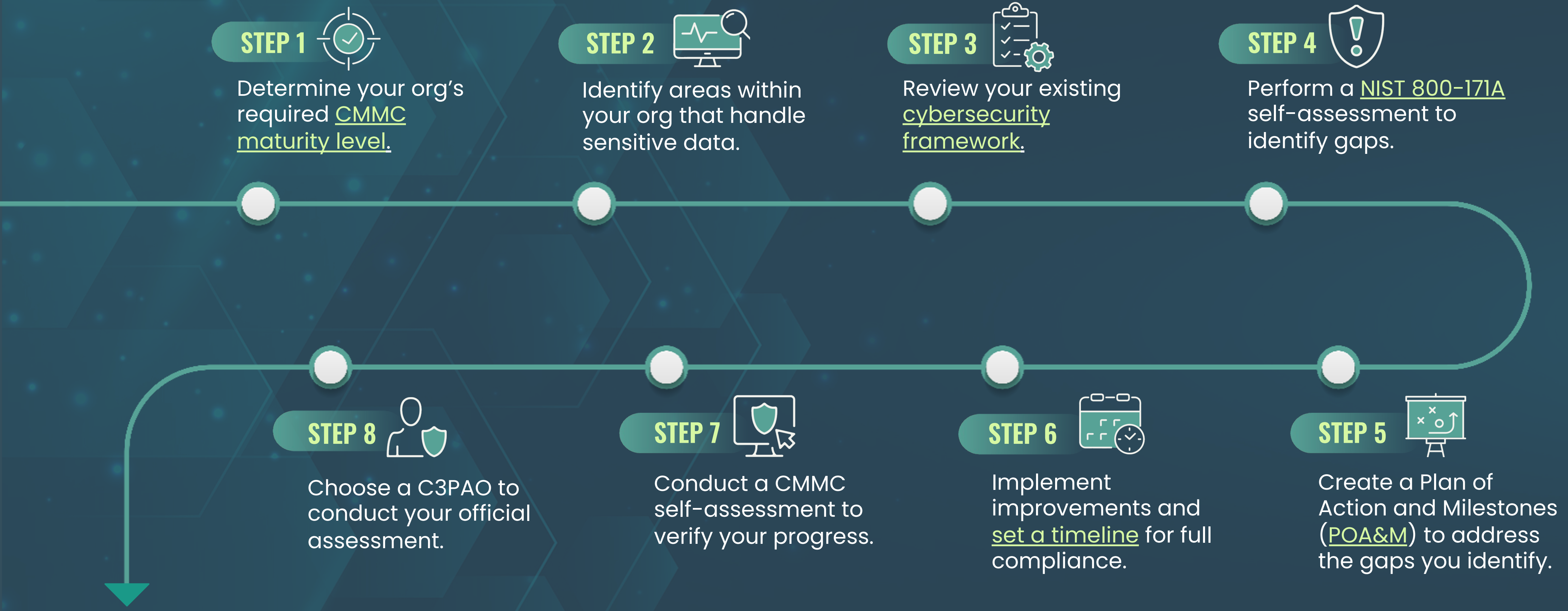
Assessors verify that teams understand and follow security processes

TEST

Technical verification to ensure security controls are working as expected

KEY TAKEAWAY: Compliance isn't just about having policies—it's about proving they work.

YOUR ROADMAP TO COMPLIANCE



STEP 1

Determine your org's required CMMC maturity level.

STEP 2

Identify areas within your org that handle sensitive data.

STEP 3

Review your existing cybersecurity framework.

STEP 4

Perform a NIST 800-171A self-assessment to identify gaps.

STEP 5

Create a Plan of Action and Milestones (POA&M) to address the gaps you identify.

STEP 6

Implement improvements and set a timeline for full compliance.

STEP 7

Conduct a CMMC self-assessment to verify your progress.

STEP 8

Choose a C3PAO to conduct your official assessment.

How ready are you? Evaluate your posture now

PLANNING YOUR ASSESSMENT

DETERMINE YOUR CMMC LEVEL

- Identify which CMMC level applies to your business
- Check if your contracts include DFARS 7012 or require Level 2 certification

CONDUCT A GAP ASSESSMENT

- Identify security weaknesses before an official audit
- Compare current practices against against NIST 800-171 requirements

DEVELOP A PLAN OF ACTION & MILESTONES (POA&M)

- Create a roadmap to close compliance gaps
- Prioritize remediation tasks based on risk and impact

NEXT UP: Moving from preparation to implementation

REMEDIATION & IMPLEMENTATION: TURNING PLANS INTO ACTIONS

PUT TOGETHER YOUR REMEDIATION TEAM

- Assign internal resources or engage external experts to drive compliance efforts

IMPLEMENT AN ACTION PLAN

- Address compliance gaps to reach a **SPRS score of 110** in alignment with NIST 800-171
- Focus on missing **policies, controls, and evidence collection** to meet requirements

DEVELOP AND MAINTAIN DOCUMENTATION

- Ensure all security measures are properly documented
- Keep records up to date to streamline the assessment process

BEGIN CONDUCTING MOCK ASSESSMENTS

- Validate readiness by simulating an actual CMMC assessment
- Your mock assessment is only as strong as the expertise behind it—consider **bringing in a third party**

PRO TIP: Link directly to your live documents within your System Security Plan (SSP) to keep everything organized and accessible.

Engage a C3PAO early—there are ~65 C3PAOs, and their availability is limited.

FINAL PREPARATION FOR YOUR CMMC ASSESSMENT

VERIFY DOCUMENTATION IS AUDIT-READY

- Ensure all policies, procedures, and security controls are documented
- Cross-check that your **System Security Plan (SSP)** is aligned with actual practices

CONDUCT AN INTERNAL MOCK ASSESSMENT AND TEST AGAINST THE THREE EVALUATION METHODS:

- **Examine:** Do policies match real-world security practices?
- **Interview:** Can your team explain and demonstrate compliance?
- **Test:** Do security controls function as required?

ADDRESS ANY GAPS BEFORE THE C3PAO REVIEW

- Review past **gap assessments** and confirm all remediation is complete
- If your C3PAO does not deem you ready, they will not proceed with the official assessment

ASSESSMENT & CERTIFICATION

Your **C3PAO will take the lead** in evaluating your compliance, reviewing documentation, and validating security controls. While timelines can vary, expect the assessment to take one full business week.

POST-ASSESSMENT PROCESS

Outbrief Meeting – Your C3PAO will provide initial findings and identify any deficiencies

Corrective Actions (if needed) – If gaps exist, you may need remediation before certification

Issuance of Certificate of Status – Upon successful completion, your **CMMC Level 2 certification** is awarded

Note: *It may take a few days before hearing back from your assessor on certification status*

PRO TIP: A **CMMC-certified third-party vendor** can help streamline the process and improve your chances of passing.

KEY TAKEAWAYS FROM OUR CMMC LEVEL ASSESSMENT

- **PREPARATION IS CRITICAL**
  A structured, well-documented approach to compliance is essential. Ensure security controls and documentation are solid **before** the formal assessment.

- **THE IMPORTANCE OF A STRONG SYSTEM SECURITY PLAN (SSP)**
  Your **SSP must be detailed, accurate, and reflect actual security practices**. Any inconsistencies will raise red flags during the assessment.

- **YOU CAN'T DO THIS WITH A PART-TIME IT DEPARTMENT**
  Achieving CMMC compliance requires **dedicated security expertise**. A small or overburdened IT team will struggle to meet the depth of requirements.

- **EVIDENCE COLLECTION TAKES TIME**
  Gathering and presenting compliance evidence (logs, policies, training records) is **a time-intensive process**. Organizations should proactively manage and track evidence **before** the assessment.

- **ONGOING COMPLIANCE IS JUST AS IMPORTANT AS INITIAL CERTIFICATION**
  CMMC is not a one-time event. Maintaining compliance requires continuous monitoring, policy updates, and periodic security reviews.

- **YOU MAY NOT HEAR FROM YOUR ASSESSOR FOR DAYS**
  The assessment process isn't always immediate. There may be **delays in feedback** as assessors review documentation and evidence. Be patient and prepared.

- **THIS IS A MUCH MORE DETAILED AUDIT COMPARED TO OTHER COMPLIANCE ASSESSMENTS**
  CMMC **goes deeper than NIST 800-171 self-attestations** or other compliance frameworks. Expect **rigorous evidence requests** and in-depth scrutiny of both policies and technical controls.

NAVIGATING NEXT STEPS

SPEAK WITH AN ADVISOR

Get expert guidance on your CMMC readiness

DOWNLOAD OUR TALK TO YOUR BOSS ABOUT CMMC DECK

Equip your team with key talking points to address CMMC compliance with managers and executives

DISCOVER YOUR CMMC READINESS SIGNAL ONLINE

Quickly assess where you stand