Vendor Readiness Guide

What you need to know and do to achieve Cybersecurity Maturity Model Certification

Prepared by AMBAC Materials | June 2026

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a DoD program requiring defense contractors to prove they protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Unlike earlier self-assessment frameworks, CMMC Level 2 requires a certified third-party audit — you cannot simply self-certify.

CMMC has three levels. If your company handles CUI under a DoD contract, you almost certainly need Level 2.

Level	Who Needs It?	# Practices	3rd-Party Audit?
Level 1 — Foundational	All DoD contractors with FCI	17	No — self-assessment
Level 2 — Advanced	Contractors handling CUI	110	Yes — C3PAO required
Level 3 — Expert	Critical CUI / high-value programs	110+	Yes — DIBCAC audit

What Counts as CUI?

Controlled Unclassified Information (CUI) is government-owned or government-generated information that must be safeguarded. Common examples in defense supply chains include:

- Technical data, drawings, and specifications for defense articles
- Export-controlled information (ITAR / EAR)
- Contract performance data and pricing information
- Engineering data related to military systems
- Personally identifiable information (PII) within government contracts

If you receive, process, store, or transmit any of the above, CMMC Level 2 applies to your systems and processes.

What Level 2 Requires

Level 2 maps directly to the 110 security practices in NIST SP 800-171 Revision 2, organized across 14 domains. The pages below walk through each domain in plain language.

The path to certification:

- Step 1: Implement all 110 practices across the 14 domains
- Step 2: Document implementation in a System Security Plan (SSP)
- Step 3: Capture any gaps in a Plan of Action & Milestones (POA&M;)
- Step 4: Engage a certified C3PAO assessor for your formal audit
- Step 5: Receive Level 2 certification (valid for 3 years)

The 14 Security Domains — Plain English

Each section below describes what the domain covers and the key things you must have in place. Use the companion Excel checklist to track your status against all 110 individual practices.

AC — Access Control	
What this means:	*Control who can access your systems, data, and networks.*
Key Requirements	
1	Maintain a list of all authorized users and devices
2	Apply least-privilege — users get only the access they need
3	Use multi-factor authentication (MFA) for privileged accounts
4	Encrypt all remote access sessions (VPN with strong encryption)
5	Lock screens automatically after inactivity
6	Disable accounts for terminated employees immediately

AT — Awareness & Training	
What this means:	*Make sure your people know the security risks and their responsibilities.*
Key Requirements	
1	Conduct annual cybersecurity awareness training for all staff
2	Train employees to recognize phishing and social engineering
3	Document and retain training completion records

AU — Audit & Accountability	
What this means:	*Keep logs of who did what on your systems, and review them.*

Key Requirements	
1	Enable audit logging on all systems that handle CUI
2	Retain logs long enough to investigate incidents
3	Review logs regularly and alert on failures
4	Protect logs from tampering or deletion

CM — Configuration Management

What this means:	*Keep systems configured securely and control what software runs.*

Key Requirements	
1	Maintain documented baseline configurations for all systems
2	Disable or remove unnecessary software, services, and ports
3	Control user-installed software — no unauthorized apps
4	Apply security patches in a timely manner

IA — Identification & Authentication

What this means:	*Verify the identity of every user and device before granting access.*
Key Requirements	
1	Enforce strong, complex passwords (minimum length + complexity rules)
2	Prohibit password reuse across generations
3	Use MFA for all privileged and remote access
4	Store passwords in hashed/encrypted form only
5	Disable inactive accounts after a defined period

IR — Incident Response

What this means:	*Have a plan to detect, respond to, and recover from cyber incidents.*
Key Requirements	
1	Document an incident response plan and test it at least annually
2	Know who to notify (DoD/government) — report within 72 hours of an incident
3	Track and document all incidents in a log

MA — Maintenance

What this means:	*Control how and when systems are maintained, especially remotely.*
Key Requirements	
1	Log all maintenance activities
2	Require MFA for remote maintenance sessions
3	Sanitize equipment before sending off-site for repair
4	Supervise maintenance personnel who lack full access authorization

MP — Media Protection	
What this means:	*Protect physical and digital media that contains CUI.*
Key Requirements	
1	Restrict access to media (USB drives, hard drives, printouts) with CUI
2	Encrypt CUI on all portable and removable media
3	Securely wipe or physically destroy media before disposal
4	Label and track CUI media throughout its lifecycle

PS — Personnel Security

What this means:	*Screen people before giving them CUI access, and act fast on staff changes.*
Key Requirements	
1	Conduct background checks before granting CUI access
2	Revoke all access immediately upon termination or role change
3	Maintain documented offboarding procedures

PE — Physical Protection

What this means:	*Control physical access to your facilities and equipment.*
Key Requirements	
1	Restrict physical entry to areas where CUI is stored or processed
2	Log all physical access (badge readers, visitor logs)
3	Escort and monitor all visitors
4	Protect against environmental hazards: fire, flood, power loss

RA — Risk Assessment

What this means:	*Regularly assess your risks and fix the vulnerabilities you find.*
Key Requirements	
1	Perform a formal risk assessment at least annually
2	Run vulnerability scans on all systems handling CUI
3	Prioritize and remediate vulnerabilities based on assessed risk

CA — Security Assessment

What this means:	*Periodically test your controls to confirm they actually work.*
Key Requirements	
1	Assess security controls periodically via internal audit or third party
2	Create a Plan of Action & Milestones (POA&M;) for any identified gaps
3	Monitor controls continuously for degradation or changes

SC — System & Communications Protection	
What this means:	*Protect the networks and communications that carry CUI.*
Key Requirements	
1	Segment networks — separate CUI systems from general/public networks
2	Use FIPS-validated encryption for CUI in transit
3	Implement a deny-by-default firewall policy
4	Use encrypted sessions for managing all network devices
5	Control and monitor remote access, VoIP, and mobile code use

SI — System & Information Integrity	
What this means:	*Keep systems clean, patched, and monitored for threats.*
Key Requirements	
1	Deploy and maintain up-to-date antivirus/EDR on all endpoints
2	Patch operating systems and applications promptly
3	Monitor systems for unusual activity and signs of attack
4	Enable spam filtering on all email gateways

Pre-Assessment Readiness Checklist

Before engaging a C3PAO for your formal audit, confirm you have the following in place. These are the most commonly cited gaps during CMMC assessments.

#	Pre-Assessment Item	Status
1	System Security Plan (SSP) — document all systems and how they are protected	[ ] Done [ ] In Progress [ ] Not Started
2	Plan of Action & Milestones (POA&M;) — list gaps and your remediation plan	[ ] Done [ ] In Progress [ ] Not Started
3	Asset inventory — every device, server, and application that touches CUI	[ ] Done [ ] In Progress [ ] Not Started
4	User access list — who has access to what, with justification	[ ] Done [ ] In Progress [ ] Not Started
5	Incident response plan — written, tested, with DoD contact procedures	[ ] Done [ ] In Progress [ ] Not Started
6	Configuration baselines documented for all CUI-touching systems	[ ] Done [ ] In Progress [ ] Not Started
7	Vulnerability scan results and evidence of remediation	[ ] Done [ ] In Progress [ ] Not Started
8	Training records — proof all staff completed cybersecurity awareness training	[ ] Done [ ] In Progress [ ] Not Started
9	MFA enabled for privileged and remote accounts	[ ] Done [ ] In Progress [ ] Not Started
10	Encryption in place for CUI at rest and in transit	[ ] Done [ ] In Progress [ ] Not Started

Next Steps & Resources

To begin your CMMC Level 2 journey:

- Review the CMMC Level 2 Vendor Assessment Checklist (provided separately) and self-assess against all 110 practices
- Download NIST SP 800-171 Rev 2: nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- Review the DoD CMMC model: dodcio.defense.gov/CMMC/
- Find an accredited C3PAO assessor: cyberab.org
- Consider a gap assessment with a cybersecurity consultant before your formal audit

Questions about CMMC requirements for AMBAC Materials vendors? Contact your AMBAC procurement representative.