ONE CIRCLE SOLUTIONS

CMMC Compliance Checklist

A practical CMMC 2.0 readiness checklist for defense contractors — the levels, scoping steps, and a family-by-family walkthrough of the NIST SP 800-171 controls behind Level 2.

Updated July 2026

If your company handles Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) for the Department of Defense, the Cybersecurity Maturity Model Certification (CMMC) program is becoming a condition of doing business. This checklist walks through what CMMC 2.0 requires, how to scope your environment, and the controls behind each level, so you can find your gaps before an assessor does.

Use it as a self-assessment starting point. It is a readiness aid, not a substitute for the official CMMC and NIST SP 800-171 documentation or a certified assessment.

What CMMC is and why it exists

CMMC is the Department of Defense's framework for verifying that companies in the Defense Industrial Base (DIB) protect sensitive government information. It exists because self-attestation alone proved unreliable, and adversaries exploited the gap by targeting smaller, less-defended suppliers.

CMMC 2.0 ties assessment rigor to the sensitivity of the information you handle. Lower-risk work allows self-assessment; work involving CUI critical to national security requires an independent, third-party assessment.

Who needs to comply

If any of the following is true, CMMC almost certainly applies to you:

- [ ] You are a prime contractor or subcontractor anywhere in the DoD supply chain.
- [ ] Your contracts include DFARS 252.204-7012 (safeguarding covered defense information and cyber incident reporting).
- [ ] You receive, store, process, or transmit Federal Contract Information (FCI).
- [ ] You handle Controlled Unclassified Information (CUI) — which triggers Level 2 or above.
- [ ] You have submitted, or must submit, a NIST SP 800-171 self-assessment score to SPRS under DFARS 252.204-7019 and 7020.

The three CMMC levels

Determine which level your contracts require before assessing anything.

- [ ] Level 1 (Foundational): 17 practices protecting FCI, based on FAR 52.204-21. Annual self-assessment and affirmation in SPRS.

- [ ] Level 2 (Advanced): 110 practices aligned with NIST SP 800-171 Rev 2, protecting CUI. Self-assessment or a triennial C3PAO third-party assessment, depending on the contract.
- [ ] Level 3 (Expert): Level 2 controls plus a subset of NIST SP 800-172, assessed by the government (DIBCAC).
- [ ] Most DIB companies handling CUI are targeting Level 2. Confirm with your contracting officer rather than guessing.

Before you start: scope your environment

Scoping is where most CMMC efforts succeed or fail.

- [ ] Identify exactly where FCI and CUI are received, stored, processed, and transmitted — email, file shares, endpoints, cloud tenants, backups.
- [ ] Define the assessment boundary and separate in-scope from out-of-scope systems, using segmentation where practical.
- [ ] Categorize assets: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, and Out-of-Scope Assets.
- [ ] Write your System Security Plan (SSP) describing your boundary, systems, and how each control is met.
- [ ] Stand up a Plan of Action and Milestones (POA&M;) to track open gaps with owners and dates.
- [ ] Confirm your current NIST SP 800-171 score in SPRS and how it was calculated (start at 110, subtract weighted points per unmet control).

Access Control (AC)

Limit system access to authorized users, processes, and devices.

- [ ] Are accounts unique per user, with role-based permissions following least privilege?
- [ ] Is privileged (admin) access separated from day-to-day accounts and tightly limited?
- [ ] Do you control and log remote access through managed, encrypted channels?
- [ ] Is CUI flow controlled between systems and access restricted on need-to-know?
- [ ] Are session locks, automatic logoff, and control of portable devices enforced?

Awareness and Training (AT)

Make sure people understand the risks and their responsibilities.

- [ ] Do all users receive security awareness training aligned to their roles?
- [ ] Are staff trained to recognize and report phishing, social engineering, and insider-threat indicators?
- [ ] Do privileged users and security staff get role-specific training beyond the baseline?
- [ ] Is training completion tracked and refreshed on a defined schedule?

Audit and Accountability (AU)

Create and retain the logs you need to detect, investigate, and prove what happened.

- [ ] Are audit logs generated across CUI systems, capturing the events you'd need in an investigation?
- [ ] Can every logged action be traced to a specific user (individual accountability)?
- [ ] Are logs protected from unauthorized access, modification, and deletion?
- [ ] Is time synchronized across systems so events can be correlated?
- [ ] Are logs reviewed regularly, with alerting on the events that matter, and retained per requirements?

Configuration Management (CM)

Establish secure baselines and control changes to them.

- [ ] Do you maintain documented, secure baseline configurations for hardware and software?
- [ ] Are changes reviewed, approved, and tracked through change control?
- [ ] Do you enforce least-functionality — disabling unnecessary ports, protocols, services, and software?
- [ ] Do you maintain an inventory of authorized software and restrict unauthorized applications?
- [ ] Are security-relevant settings enforced and monitored for drift?

Identification and Authentication (IA)

Verify the identity of users and devices before granting access.

- [ ] Is multi-factor authentication enforced for privileged accounts and network/remote access?
- [ ] Are password/authenticator policies enforced and cryptographically protected?
- [ ] Are shared or generic accounts eliminated, or tightly controlled where unavoidable?
- [ ] Are devices identified and authenticated before connecting to in-scope systems?
- [ ] Are temporary and default credentials changed before systems go into use?

Incident Response (IR)

Be ready to detect, respond to, and report incidents — including the 72-hour rule.

- [ ] Do you have a documented incident response plan with defined roles and escalation paths?
- [ ] Can you report cyber incidents to DoD within 72 hours per DFARS 252.204-7012?
- [ ] Do you test the plan (e.g. tabletop exercises) and update it from lessons learned?
- [ ] Are detection and monitoring in place to identify incidents in the first place?
- [ ] Is there a process to preserve evidence and support forensic analysis?

Maintenance (MA)

Perform maintenance in a controlled way that doesn't create new exposure.

- [ ] Is maintenance — including remote maintenance — scheduled, controlled, and logged?
- [ ] Are maintenance tools and media checked for malicious code before use?
- [ ] Is media sanitized of CUI before equipment leaves your control?
- [ ] Are maintenance personnel supervised, with access appropriately restricted?

Media Protection (MP)

Protect CUI on digital and physical media in use, storage, and disposal.

- [ ] Is media containing CUI marked, and access limited to authorized users?
- [ ] Is CUI encrypted on portable devices and removable media?
- [ ] Is media sanitized or destroyed before disposal or reuse, using approved methods?
- [ ] Is the use of removable media controlled, and prohibited where not needed?
- [ ] Is CUI protected during transport outside controlled areas?

Personnel Security (PS)

Manage the risk that comes with the people who have access.

- [ ] Are individuals screened before being granted access to CUI systems?
- [ ] Is access promptly revoked on termination or role change (same-day for departures)?
- [ ] Are CUI systems protected during personnel transfers and reassignments?

Physical Protection (PE)

Control physical access to systems, equipment, and environments holding CUI.

- [ ] Is physical access to facilities and equipment limited to authorized individuals?
- [ ] Are visitors escorted, logged, and their activity monitored?
- [ ] Are physical access devices (keys, badges) managed and audited?
- [ ] Is CUI protected at alternate and remote work sites, including home offices?

Risk Assessment (RA)

Understand your risks and vulnerabilities so you can prioritize fixes.

- [ ] Do you assess risk to operations and assets from CUI systems on a defined cadence?
- [ ] Do you scan for vulnerabilities regularly and when new ones are announced?
- [ ] Are identified vulnerabilities remediated based on risk and tracked to closure?

- [ ] Do risk assessments inform your POA&M; and security roadmap?

Security Assessment (CA)

Verify that your controls actually work, and manage the gaps that remain.

- [ ] Do you periodically assess your controls to confirm they're effective?
- [ ] Is your System Security Plan current and reflective of the real environment?
- [ ] Is your POA&M; actively managed, with realistic milestones and owners?
- [ ] Do you monitor controls on an ongoing basis, not only at assessment time?

System and Communications Protection (SC)

Protect information in transit and at the boundaries of your systems.

- [ ] Is CUI encrypted in transit using FIPS-validated cryptography?
- [ ] Are network boundaries monitored and controlled, deny-by-default at perimeters?
- [ ] Is your network architected to separate CUI systems from general-purpose and public-facing ones?
- [ ] Are cryptographic keys managed securely, and mobile code and collaboration tools controlled?
- [ ] Is CUI encrypted at rest where required?

System and Information Integrity (SI)

Find and fix flaws, and detect malicious activity, in a timely way.

- [ ] Are flaws and vulnerabilities identified and patched within defined timeframes?
- [ ] Is malicious-code protection deployed, updated, and monitored across endpoints?
- [ ] Do you monitor systems and network traffic for attacks and indicators of compromise?
- [ ] Do you act on security alerts and advisories relevant to your environment?
- [ ] Is 24/7 monitoring in place, or is there a gap outside business hours?

Common gaps we see

In first-time CMMC readiness reviews, the same shortfalls come up again and again:

- [ ] No clear CUI boundary — the whole company is treated as in-scope, ballooning cost and effort.
- [ ] MFA deployed for email but not for all remote and privileged access.
- [ ] Logging enabled but never reviewed — no monitoring, no alerting, no one watching after hours.
- [ ] An SSP that describes an idealized environment, not the one that actually exists.
- [ ] A POA&M; that hasn't been touched since it was created.
- [ ] Encryption in place, but not FIPS-validated where the requirement demands it.

From checklist to certification

Working through this checklist tells you roughly where you stand. Turning that into a defensible assessment result means closing gaps in a deliberate order, generating the evidence assessors expect, and keeping the controls operating — not just implemented once.

One Circle Solutions helps defense contractors get there: a scoped gap assessment against NIST SP 800-171, a prioritized remediation roadmap, the monitoring and logging the framework assumes you run, and support through the assessment itself.

Ready to get CMMC-ready? One Circle Solutions runs scoped NIST SP 800-171 gap assessments, builds the remediation roadmap, and operates the monitoring the framework assumes you have. Start at onecs.net/contact.