CMMC 2.0 Level 2 Readiness Checklist

For Utah and East Tennessee defense contractors preparing for CMMC 2.0 Level 2 assessment under NIST SP 800-171 Rev. 2.

Gravity Networks

Salt Lake City, UT · Knoxville, TN
gogravity.net · 855-444-6500

MAY 2026

CMMC 2.0 Level 2 Readiness Checklist

A working checklist for Utah and East Tennessee defense contractors preparing for CMMC 2.0 Level 2. Built around NIST SP 800-171 Rev. 2, the framework the DoD uses to evaluate your cybersecurity posture.

Published by Gravity Networks · gogravity.net · Salt Lake City, UT · Knoxville, TN

How to use this checklist

This document is the working version of the readiness review we walk every CMMC client through before any implementation work begins. It maps the 110 controls in NIST SP 800-171 Rev. 2 into 14 families, with short checks and notes for the items most SMB defense contractors get wrong.

It is **not** an official CMMC scoring tool. Use it to surface gaps internally before paying for an external assessment, and to align your IT lead, your information-security owner, and your legal/contracts function on what needs to happen first.

Mark each item:

- **Y** — Fully implemented, evidence available
- **P** — Partially implemented (POA&M item)
- **N** — Not implemented
- **N/A** — Not applicable, with documented reasoning

A defensible Level 2 self-assessment requires the answer to be Y or documented in the POA&M; "we will get to it" is not an acceptable answer to a C3PAO.

1. Pre-assessment scoping

Before any control work, you must define what's in scope. Most CMMC engagements fail because the scope was assumed rather than mapped.

- ☐ **Identified every form of CUI handled by the business** (engineering drawings, technical specs, program documentation, export-controlled data, etc.)
- ☐ **Documented where CUI enters the environment** (email, SFTP, prime contractor portals, physical media)
- ☐ **Documented where CUI is stored** (file shares, SharePoint, engineering workstations, removable media, archive systems)

- [ ] **Documented how CUI flows internally** (who accesses it, what apps process it, what external systems integrate)
- [ ] **Documented where CUI exits** (reports back to prime, customer deliverables, archival, destruction)
- [ ] **Identified all CUI-handling personnel** (engineers, admins, contracts staff, IT staff with access)
- [ ] **Identified all third-party providers with CUI access** (cloud services, IT vendors, contractors)
- [ ] **Defined the assessment boundary** (full tenant or segmented CUI enclave)
- [ ] **Data-flow diagram completed and approved by leadership**

> **Common gotcha:** Many SMB DIB contractors treat ALL their business data as if it's CUI. It's not. A precise scope drives precise (and cheaper) implementation. A loose scope drives expensive over-engineering.

---

2. Access Control (AC) — 22 controls

- [ ] Unique user accounts for every individual (no shared logins)
- [ ] Documented role-based access policy with periodic reviews (quarterly recommended)
- [ ] Multi-factor authentication enforced on **all** CUI-touching access
- [ ] Phishing-resistant MFA (hardware key / Passkey) for privileged and admin accounts
- [ ] Conditional access policies block legacy authentication protocols
- [ ] Session timeouts configured per NIST baseline (typically 15 minutes inactive)
- [ ] Account lockout thresholds enforced after failed attempts
- [ ] Privileged accounts separated from regular user accounts (admins have two accounts)
- [ ] Remote access via VPN with MFA, full-tunnel, logged
- [ ] Wireless networks segmented from CUI environment

> **Common gotcha:** MFA on email but not on the VPN, or on user accounts but not service accounts. The audit asks "all" — make it actually be all.

---

3. Awareness and Training (AT) — 3 controls

- [ ] Security awareness training delivered to all CUI-handling personnel at hire
- [ ] Annual security refresher training tracked with completion records
- [ ] Privileged-user training covering admin-level threats (above the baseline)

- [ ] Phishing simulations on a documented cadence (monthly minimum for privileged users)
- [ ] Records retention for all training completions (audit-accessible)

> **Common gotcha:** Training was conducted, but the records aren't recoverable. If you can't show who completed what and when, the assessor scores it as not implemented.

---

4. Audit and Accountability (AU) — 9 controls

- [ ] Centralized logging deployed across CUI-handling systems
- [ ] Logs include user authentication, privileged operations, file access on CUI repositories
- [ ] Log retention period defined (90 days online, longer archive — assessor-readable)
- [ ] Time synchronization across all logged systems (NTP)
- [ ] Log review process documented with named owners
- [ ] Audit log access restricted to authorized roles
- [ ] Logs protected from unauthorized modification
- [ ] Failed audit event response procedure documented

> **Common gotcha:** "Our server writes to event log" is not centralized logging. SIEM or equivalent aggregation is the bar.

---

5. Configuration Management (CM) — 9 controls

- [ ] Baseline configurations documented for every system class (workstations, servers, network devices)
- [ ] Change control process documented and followed for production changes
- [ ] Software inventory maintained — installed software approved before deployment
- [ ] Removable media controls in place (USB blocked or whitelisted at policy level)
- [ ] Mobile device management (MDM) for any device accessing CUI
- [ ] Application whitelisting or equivalent on CUI-touching endpoints
- [ ] Default credentials changed on every device and application
- [ ] Unused services and ports disabled per baseline

Common gotcha: Baselines exist on paper but drift in practice. Implement configuration enforcement (Intune, Group Policy, etc.) so drift is detected.

---

6. Identification and Authentication (IA) — 11 controls

- ☐ Identity proofing for new account creation
- ☐ Password complexity meeting NIST 800-63B (length over complexity)
- ☐ Password rotation policies (annual minimum, immediate on compromise)
- ☐ Account lockout after failed authentication attempts
- ☐ Privileged accounts require MFA without exception
- ☐ Service accounts inventoried and rotated regularly
- ☐ Shared accounts eliminated or specifically justified and logged
- ☐ Credentials transmitted only over encrypted channels

Common gotcha: A few service accounts with non-expiring passwords used for legacy app integration. These are the holes attackers find.

---

7. Incident Response (IR) — 3 controls

- ☐ Written Incident Response Plan covering detection, containment, eradication, recovery, lessons learned
- ☐ Incident response team defined with named primary and backup
- ☐ Annual incident response tabletop exercise conducted with leadership
- ☐ Incident reporting procedures defined (internal escalation, customer/prime notification, regulator obligations)
- ☐ Records of past incidents retained per policy

Common gotcha: Plan exists but nobody on the team has read it in 18 months. Run the tabletop annually so the plan reflects reality.

8. Maintenance (MA) — 6 controls

- ☐ Patch management cadence documented (security patches within 30 days)
- ☐ Maintenance personnel access logged and authorized
- ☐ Off-site maintenance follows defined procedures (sanitization before/after)
- ☐ Maintenance tools controlled (no unauthorized utilities introduced)
- ☐ Records of maintenance activities retained

9. Media Protection (MP) — 9 controls

- ☐ Removable media containing CUI marked, controlled, and inventoried
- ☐ Sanitization procedures for media containing CUI before reuse or disposal
- ☐ Encrypted at rest on all media (BitLocker, FileVault, or equivalent)
- ☐ Physical security for media in transit
- ☐ Backup media subject to same protections as production CUI
- ☐ Cryptographic mechanisms approved (FIPS 140-2 / 140-3 validated for CUI)

10. Personnel Security (PS) — 2 controls

- ☐ Background screening for CUI-handling personnel
- ☐ Access termination procedures (immediate revocation on departure)
- ☐ Records of personnel actions (hire, role change, departure) maintained

Common gotcha: Person leaves, IT removes their account, but they still have a registered MFA token and an unrevoked OAuth grant in M365. Termination has to be holistic.

11. Physical Protection (PE) — 6 controls

- ☐ Physical access to CUI-storing facilities controlled (key card, log)
- ☐ Visitor access controlled, escorted, logged
- ☐ Physical access logs reviewed periodically

- [ ] Monitoring of physical access (camera, alarm)
- [ ] Maintenance personnel escorted in CUI areas

12. Risk Assessment (RA) — 3 controls

- [ ] Periodic risk assessments documented (annual minimum)
- [ ] Vulnerability scans on cadence (monthly minimum)
- [ ] Risk register maintained with treatment decisions and named owners
- [ ] Threat intelligence sources monitored (CISA advisories, sector-specific feeds)

13. Security Assessment (CA) — 4 controls

- [ ] Self-assessment of controls performed and documented
- [ ] System Security Plan (SSP) maintained, current, approved
- [ ] Plan of Action & Milestones (POA&M) maintained with target dates
- [ ] Continuous monitoring strategy documented and active
- [ ] Periodic re-assessment of controls (annually at minimum, after major changes)

14. System and Communications Protection (SC) — 16 controls

- [ ] Boundary protection (firewalls, segmentation between CUI enclave and other networks)
- [ ] Encryption in transit (TLS 1.2+ on all CUI flows)
- [ ] Encryption at rest on all CUI storage
- [ ] Cryptographic key management documented
- [ ] Mobile code (ActiveX, Java applets, etc.) controlled per policy
- [ ] VoIP usage assessed for CUI-handling risk
- [ ] DNS protection (filtering, secure resolvers)
- [ ] Cloud services formally authorized before CUI flows through them
- [ ] Email protection (SPF, DKIM, DMARC, anti-phishing)
- [ ] Session security (encryption, integrity, authentication)

15. System and Information Integrity (SI) — 7 controls

- [ ] Endpoint detection and response (EDR) on every CUI-touching system
- [ ] Anti-malware controls with current signatures
- [ ] System monitoring for unauthorized changes
- [ ] Vulnerability remediation cadence per RA family
- [ ] Spam and phishing protection on email
- [ ] Information input validation on applications handling CUI
- [ ] Error handling that doesn't leak sensitive information

> **Common gotcha:** Traditional antivirus is not enough for Level 2. EDR with behavioral detection is the bar.

16. Documentation deliverables

These are the documents an assessor will ask for. Build them as you implement controls — not at the end.

- [ ] **System Security Plan (SSP)** — describes how each of the 110 controls is implemented in your environment. Living document, updated quarterly. Plain English.
- [ ] **Plan of Action & Milestones (POA&M)** — list of controls not fully implemented with named owners and target dates.
- [ ] **Data-flow diagram** — visual of how CUI moves through the business.
- [ ] **Network diagram** — segmentation, firewalls, the CUI enclave boundary.
- [ ] **Asset inventory** — every system that stores, processes, or transmits CUI.
- [ ] **Risk register** — identified risks, treatment decisions, owners.
- [ ] **Incident response plan** — written, exercised annually.
- [ ] **Training records** — who completed what training when.
- [ ] **Change control records** — production changes logged with approvals.
- [ ] **Vulnerability scan reports** — most recent results plus remediation history.
- [ ] **Backup and restore test logs** — proof that backups actually restore.

17. Pre-assessment activities

- [ ] **Internal pre-assessment** — walk all 110 controls against your environment and evidence. Document gaps in POA&M.
- [ ] **Score self-assessment for SPRS** — calculate the score per the DoD methodology and post it. Re-post when material changes occur.
- [ ] **Mock assessment by an independent reviewer** — someone outside the implementation team walks your SSP as though they were the C3PAO. Find the gaps now, not in front of the real assessor.
- [ ] **Tabletop exercise** — run a realistic incident scenario with leadership in the room. Document outcomes.
- [ ] **Final SSP and POA&M review** — leadership sign-off before submission.

What "ready" actually looks like

A Level 2-ready environment has been operating at the control bar for **at least 90 days** before the assessment. Controls assembled the week before don't satisfy a C3PAO — the assessor looks for evidence of sustained operation, not snapshots.

If you're under that 90-day mark and the assessment is approaching, prioritize:

1. **Get the technical control stack running** (EDR, SOC, MFA, logging, encryption — these score the most points in the SPRS rubric and are fastest to deploy).
2. **Write the SSP in parallel** with implementation — don't wait.
3. **Move what you can to POA&M** with realistic target dates — assessors accept POA&M items for non-critical gaps.
4. **Talk to your prime** — many will grant a documented remediation extension if you have a credible POA&M with a timeline.

Who Gravity Networks helps

We run CMMC engagements end-to-end for Utah and East Tennessee defense contractors — DIB manufacturers around Hill AFB, engineering and technical services firms in the Oak Ridge ecosystem, IT-services subcontractors holding their own Level 2 obligation.

Gap assessment → CUI enclave architecture → control deployment → SSP & POA&M → mock assessment → ongoing operation. Same team, one phone number, two metros.

Talk to us about a scoping call: - **Salt Lake City office** — 350 S 200 E, Suite 102, Salt Lake City, UT 84111 · 801-590-2637 - **Knoxville office** — 8351 E. Walker Springs Lane Ste 302, Knoxville, TN 37923 · 865-934-9900 - **Toll-free** — 855-444-6500 - **Email** — info@gogravity.net - **Online** — gogravity.net/services/cmmc-compliance/

This document is provided for informational purposes only. It is not legal, compliance, or assessment advice. Authoritative CMMC and NIST SP 800-171 Rev. 2 references should always be consulted directly. Last updated: May 2026.