anchor@anchor-cyber:~$ cat cmmc-2-practice-areas.md

ANCHOR CYBER SECURITY LLC

# CMMC 2.0 Practice Areas

Cybersecurity Maturity Model Certification 2.0 — 14 domains, three levels, and NIST SP 800-171 Rev 2 alignment. Required for DoD contractors handling FCI or CUI.

$ cmmc --levels

## Maturity Levels

### Level 1

**Foundational**

Protects Federal Contract Information (FCI). Based on FAR clause 52.204-21. Annual self-assessment with senior official affirmation.

17 practices

### Level 2

**Advanced**

Protects Controlled Unclassified Information (CUI). Aligned to NIST SP 800-171 Rev 2. C3PAO assessment required for critical programs; self-assessment for non-critical.

110 practices

### Level 3

**Expert**

Highest-risk CUI programs. Based on NIST SP 800-172 (adds 24 practices beyond Level 2). DIBCAC government-led assessment required.

134 practices

$ cmmc --domains

## 14 Practice Domains — NIST SP 800-171 Rev 2 alignment

Level 2 maps 1-to-1 with the 110 security requirements across 14 families in NIST SP 800-171 Rev 2. Each domain contains multiple practices; Level 1 draws a subset from six of these domains.

| ABBR | DOMAIN | NIST SECTION | KEY FOCUS AREAS |
|---|---|---|---|
| AC | **Access Control** | § 3.1 | Least privilege, remote access, account management, CUI flow control |
| AT | **Awareness & Training** | § 3.2 | Security awareness, role-based training, insider threat awareness |
| AU | **Audit & Accountability** | § 3.3 | Audit log creation, protection, review, and retention |
| CM | **Configuration Management** | § 3.4 | Baseline configs, change control, least functionality, deny-by-default |
| IA | **Identification & Authentication** | § 3.5 | MFA for privileged/remote access, password complexity, device authentication |
| IR | **Incident Response** | § 3.6 | IR capability, incident tracking, testing, and reporting to DoD |
| MA | **Maintenance** | § 3.7 | Controlled maintenance, sanitization of media removed for maintenance |
| MP | **Media Protection** | § 3.8 | CUI media access, transport, sanitization, and disposal |
| PS | **Personnel Security** | § 3.9 | Screening, termination/transfer procedures for CUI-handling roles |
| PE | **Physical Protection** | § 3.10 | Facility access controls, visitor management, physical protection of CUI |
| RA | **Risk Assessment** | § 3.11 | Periodic risk assessments, vulnerability scanning, remediation prioritization |
| CA | **Security Assessment** | § 3.12 | System security plan, controls assessment, plan of action & milestones (POA&M) |
| SC | **System & Comms Protection** | § 3.13 | Network segmentation, CUI encryption in transit, boundary protection |
| SI | **System & Info Integrity** | § 3.14 | Malware protection, security alerts, patching, anomaly detection |

$ cmmc --assessment-path

## Assessment Requirements by Level

LEVEL 1

### Annual Self-Assessment

Company performs and affirms results. Senior official certifies annually in SPRS (Supplier Performance Risk System). Score uploaded to SPRS.

LEVEL 2 — NON-CRITICAL

### Triennial Self-Assessment

Company performs assessment and senior official certifies every 3 years. Score in SPRS. Applies to programs DoD designates non-critical.

LEVEL 2 — CRITICAL PROGRAMS

### Triennial C3PAO Assessment

CMMC Third-Party Assessor Organization (C3PAO) conducts assessment. Certification valid 3 years. Required for contracts handling CUI in critical programs.

LEVEL 3

### Triennial DIBCAC Assessment

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) — a government body — conducts assessment. Must pass Level 2 C3PAO first.

$ cmmc --key-docs

## Primary Sources — all free from DoD and NIST

All CMMC and NIST source documents are publicly available at no cost. ISO standards are not referenced by CMMC.

| DOCUMENT | SOURCE | PURPOSE |
|---|---|---|
| **CMMC Model v2.0** | DoD / dodcio.defense.gov | Definitive model document; practice and process requirements by level |
| **NIST SP 800-171 Rev 2** | csrc.nist.gov | 110 CUI protection requirements = Level 2 practices |
| **NIST SP 800-171A** | csrc.nist.gov | Assessment procedures for 800-171 — the how-to-assess companion |
| **NIST SP 800-172** | csrc.nist.gov | Enhanced requirements for high-value CUI — Level 3 additions |
| **NIST SP 800-171 Rev 3** | csrc.nist.gov | Upcoming revision — monitor for incorporation into CMMC model |

Sources: CMMC Model v2.0, NIST SP 800-171 Rev 2, 32 CFR Part 170 (Final Rule). Anchor Cyber Security LLC.

exit 0