BEACON

by Canopy Harbor LLC

CMMC / NIST SP 800-171 Company Readiness Checklist

Version 1.0 · 2026-09-22

For modern cloud and hybrid defense contractors preparing for CMMC Level 2 (CUI) and related DFARS / 32 CFR Part 170 obligations.

Disclaimer: Educational orientation only. **Not** legal advice, not an assessment, and not a substitute for official DoD CMMC documentation, NIST publications, or qualified assessor guidance.

1. Company readiness snapshot

Mark Yes / Partial / No. Capture owners in your tracker.

Contracts & data

Item	Y	P	N	Owner / notes
DoD / DIB contracts involving FCI or CUI identified	■	■	■	_____
Clauses reviewed: DFARS 252.204-7012, -7019, -7020, -7021 (as applicable)	■	■	■	_____
CUI categories and marking guidance understood	■	■	■	_____
Flow-down to subcontractors / SaaS mapped	■	■	■	_____

Scope & architecture

Item	Y	P	N	Owner / notes
Draft CMMC Assessment Scope (enclave vs enterprise)	■	■	■	_____
Asset inventory started (endpoints, identities, cloud, OT/IoT)	■	■	■	_____
CUI data flows documented	■	■	■	_____
ESP / CSP list with shared-responsibility notes	■	■	■	_____

Governance

Item	Y	P	N	Owner / notes
Executive sponsor and affirming official identified	■	■	■	_____
Security / IT / contracts RACI drafted	■	■	■	_____
Budget and timeline assumptions socialized	■	■	■	_____
Decision: Level 1 vs Level 2 Self vs Level 2 C3PAO	■	■	■	_____

2. NIST SP 800-171 control families — evidence reminders

CMMC Level 2 aligns to NIST SP 800-171 Revision 2 (32 CFR Part 170). Use NIST SP 800-171A objectives for evidence. Rev. 3 exists at NIST but is not the CMMC Level 2 baseline until DoD incorporates it.

Family	Evidence reminders	Status
Access Control (AC)	Entra ID / IdP, Conditional Access, privileged reviews, VPN / ZTNA.	■ Met ■ Partial ■ Gap
Awareness & Training (AT)	Curriculum, completion records, phishing simulations, CUI handling.	■ Met ■ Partial ■ Gap
Audit & Accountability (AU)	Sentinel / SIEM, Defender, Intune audit, retention policy.	■ Met ■ Partial ■ Gap
Configuration Management (CM)	Intune / Autopilot baselines, IaC, CMDB, change tickets.	■ Met ■ Partial ■ Gap
Identification & Authentication (IA)	MFA registration, phishing-resistant auth, service accounts.	■ Met ■ Partial ■ Gap
Incident Response (IR)	IR plan, tabletops, DFARS 72-hour / DIBNet readiness.	■ Met ■ Partial ■ Gap
Maintenance (MA)	Vendor access procedures, JIT admin.	■ Met ■ Partial ■ Gap
Media Protection (MP)	Removable media policy, BitLocker, disposal certificates.	■ Met ■ Partial ■ Gap
Personnel Security (PS)	HR offboarding, access revocation SLAs.	■ Met ■ Partial ■ Gap
Physical Protection (PE)	Badge logs, visitor policy, colo / cloud shared-responsibility notes.	■ Met ■ Partial ■ Gap
Risk Assessment (RA)	Risk register, vuln findings, risk acceptances.	■ Met ■ Partial ■ Gap
Security Assessment (CA)	Living SSP, control assessments, POA&M; tracker.	■ Met ■ Partial ■ Gap
System & Communications Protection (SC)	TLS, SaaS Conditional Access, encryption settings.	■ Met ■ Partial ■ Gap
System & Information Integrity (SI)	EDR coverage, patch SLAs, alert runbooks.	■ Met ■ Partial ■ Gap

3. Journey milestones (outline — not a schedule promise)

Discover scope. Contracts, CUI/FCI touchpoints, asset & identity boundaries, ESP/CSP list.

Gap assessment. Map 800-171 Rev. 2 + 800-171A objectives; score honestly; seed POA&M.;

Remediate. Prioritize MFA, logging, encryption, admin boundaries, endpoint hygiene.

Document. SSP, policies, diagrams, evidence index; maintain POA&M.;

Mock assess. Dry-run using assessment objectives; fix evidence gaps.

Official path. SPRS / affirmation where required; C3PAO when contracts require Level 2 certification assessment.

Maintain. Continuous monitoring, annual affirmations, change management for scope creep.

4. Documentation pack checklist

Item	Y	P	N	Owner / notes
System Security Plan (SSP) covering assessment scope	■	■	■	_____
Network / identity / data-flow diagrams	■	■	■	_____
Policies & procedures mapped to practiced controls	■	■	■	_____
POA&M; with owners, residual risk, closure criteria	■	■	■	_____
Evidence index tied to assessment objectives	■	■	■	_____
Incident response plan + cyber incident reporting contacts	■	■	■	_____
Vendor / CSP shared-responsibility / CRM excerpts	■	■	■	_____
SPRS score / assessment result tracking process	■	■	■	_____

5. Modern environment notes

Entra ID Conditional Access and MFA; Intune compliance; Azure / M365 logging into a reviewable store; clear SaaS boundaries; privileged access / JIT admin; secrets and service principals inventoried. Cloud shifts where evidence lives—it does not remove responsibility.

Official starting points

DoD CMMC: https://dodcio.defense.gov/CMMC/
NIST SP 800-171 Rev. 2: https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
NIST SP 800-171A: https://csrc.nist.gov/pubs/sp/800/171/a/final
32 CFR Part 170: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
DFARS 252.204-7012: https://www.acquisition.gov/dfars/252.204-7012
DFARS 252.204-7021: https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7021
Cyber AB: https://cyberab.org/