COMPLIANCE CHECKLIST

CMMC 2.0 compliance checklist

Cybersecurity Maturity Model Certification 2.0

Jurisdiction: US Department of Defense supply chain

Programme details

ORGANISATION NAME

[Organisation name]

ASSIGNED TO

[Assigned to]

TARGET COMPLETION DATE

[Target completion date]

REVIEWED BY

[Reviewed by]

REVIEW DATE

[Date]

Who CMMC 2.0 applies to

Defense Industrial Base (DIB) contractors and subcontractors that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) under DFARS clauses 252.204-7012 / 7019 / 7020 / 7021.

CMMC 2.0 checklist

STEP 1

- [ ] Confirm the CMMC level required by your contract (Level 1, 2, or 3) and the relevant DFARS clause.

STEP 2

- [ ] Define the CMMC assessment scope - the people, processes, and IT assets that touch FCI or CUI.

STEP 3

- [ ] Inventory FCI and CUI flows, including third-party / cloud handling.

STEP 4

- [ ] Author the System Security Plan (SSP) documenting how each control is implemented.

STEP 5

- [ ] Self-assess against NIST SP 800-171 (Level 2) or NIST SP 800-172 (Level 3).

STEP 6

- [ ] Track Plan-of-Action-and-Milestones (POA&M) items for any temporary gaps.

STEP 7

- [ ] Submit your SPRS score in the DoD Supplier Performance Risk System.

STEP 8

- [ ] For Level 2 / 3: select an accredited C3PAO and undergo the assessment.

STEP 9

- [ ] Receive the Certificate of CMMC Status and maintain affirmation cadence.

STEP 10

- [ ] Continuously monitor changes - controls drift, scope changes, supply-chain dependencies.

FAQ

What are the CMMC 2.0 levels?

CMMC 2.0 has three levels. Level 1 (Foundational) covers the 15 basic safeguarding requirements for FCI in FAR 52.204-21(b)(1) - earlier CMMC materials sometimes expressed these as 17 practices before the count was reconciled with the FAR in 32 CFR Part 170. Level 2 (Advanced) implements the 110 NIST SP 800-171 controls for CUI. Level 3 (Expert) adds a subset of NIST SP 800-172 controls for the most sensitive CUI. The required level is dictated by the contract.

Do I need a C3PAO assessment?

Level 1 is self-assessed and self-attested. Level 2 may be self-assessed for some contracts but requires a C3PAO third-party assessment for others. Level 3 always requires a government-led DIBCAC assessment. The contract clause determines which path applies.

When does CMMC 2.0 take effect?

DoD published the final CMMC Program rule (32 CFR Part 170) on 15 October 2024, effective 16 December 2024. The companion DFARS acquisition rule (48 CFR) was published on 10 September 2025 and took effect on 10 November 2025 - that's when contracting officers began including CMMC requirements in solicitations. Phase-in through 2027-2028. Contractors should plan for assessment readiness in line with their contract award dates and the DFARS clause 252.204-7021 phase-in schedule.

How long does CMMC certification last?

Three years, with annual affirmations required during that period to confirm continued compliance with the assessed CMMC level.

How does this checklist help if our scope is still unclear?

Most CMMC programmes fail at the scoping step - too broad and you over-engineer; too narrow and the assessor expands it. The process map on this page positions scoping as the explicit gate that everything else depends on, so you can show your assessment team the assumption you're working under before authoring the SSP.

Source: https://ba-copilot.com/compliance/cmmc-compliance-checklist. Tick each item as it is completed and add the named owner.