THE CMMC READINESS CHECKLIST · 2026

You're not too small to be a target.
You're just easier.

Attackers and the Department of Defense are asking the same question about mid-market suppliers: can you show your controls work? This brief gives you a ten-point self-check, the difference between readiness and certification, and the three questions to ask before a prime asks them for you.

88%
of breaches at small and mid-sized firms involved ransomware (Verizon DBIR, 2025)

110
NIST SP 800-171 requirements behind CMMC Level 2

Nov 10, 2025
CMMC requirements began phasing into DoD contracts (DFARS rule)

01 · WHY "EASIER" IS THE REAL RISK

Size doesn't hide you. Weak controls find you.

Automated attacks don't check headcount. They look for an unpatched VPN, a reused password, or an account without MFA. A 120–person machine shop with CUI on a shared drive is easier to reach than its prime, and often connected to it.

CMMC turns that exposure into a contract question. Since the DFARS rule took effect on November 10, 2025, the required CMMC level is being written into solicitations in phases. If you handle Controlled Unclassified Information, the question is moving from "are you compliant?" to "show us."

LEVEL	APPLIES TO	REQUIREMENTS	HOW IT'S ASSESSED
Level 1	Federal Contract Information	15 basic safeguarding requirements (FAR 52.204–21)	Annual self-assessment and affirmation
Level 2	Controlled Unclassified Information	110 requirements, NIST SP 800–171 Rev. 2	Self-assessment or certified third party (C3PAO), every three years, depending on the contract
Level 3	Highest-priority CUI programs	Level 2 plus selected NIST SP 800–172 requirements	Government assessment (DIBCAC)

Readiness is not certification.

A readiness review tells you where you stand. Only a self-assessment you can defend, a C3PAO, or DIBCAC, depending on your level, produces a CMMC status. Be wary of anyone who promises certification or a fixed timeline before scoping your environment.

Readiness is not certification. This brief is not legal advice.

02 · THE TEN-POINT SELF-CHECK

Score yourself honestly. An assessor will.

Yes = 2 · Partly = 1 · No = 0. Total out of 20.

01	**Scope** We can name every system, person, and vendor that stores, processes, or transmits CUI.	☐ Yes ☐ Partly ☐ No
02	**Identity** MFA is enforced for remote, privileged, and network access to systems in scope.	☐ Yes ☐ Partly ☐ No
03	**Documentation** A current System Security Plan describes how each of the 110 NIST SP 800–171 requirements is met.	☐ Yes ☐ Partly ☐ No
04	**SPRS** Our SPRS score is submitted, current, and backed by evidence we could show an assessor.	☐ Yes ☐ Partly ☐ No
05	**Gaps** Open gaps sit on a POA&M with an owner and a target date.	☐ Yes ☐ Partly ☐ No
06	**Endpoints** Laptops and servers in scope are encrypted, patched on a schedule, and centrally managed.	☐ Yes ☐ Partly ☐ No
07	**Logging** Security logs are collected, reviewed, and retained, not just switched on.	☐ Yes ☐ Partly ☐ No
08	**Incidents** Our incident plan has been exercised, and we know how to report a cyber incident to DoD within 72 hours.	☐ Yes ☐ Partly ☐ No
09	**Recovery** We have restored from backup in the last quarter, not just confirmed backups ran.	☐ Yes ☐ Partly ☐ No
10	**Supply chain** Subcontractors, MSPs, and cloud services that touch CUI meet the requirements we flow down to them.	☐ Yes ☐ Partly ☐ No

SCORE	WHAT IT USUALLY MEANS
17–20	Solid base. Confirm it with a formal gap assessment against all 110 requirements.
10–16	Gaps an assessor will find. Usually documentation, logging, and supply-chain evidence.
0–9	Exposed to attackers and contract risk. Start with scope, MFA, and recovery.

Readiness is not certification. This brief is not legal advice.

03 · WHAT TO DO NEXT

Find out where you stand before a prime asks.

STEP	WHAT HAPPENS
See	Quantify security, compliance, and downtime exposure for your industry and headcount with the IT Risk Report.
Scope	Map where CUI lives. Shrinking scope is often the cheapest control you will ever buy.
Close	Work the POA&M: identity, endpoint, logging, and recovery controls with evidence attached.
Assess	Self-assess or engage a C3PAO, as your contract requires. Your provider prepares you; the assessor decides.

ASK IN YOUR NEXT LEADERSHIP MEETING

1. If a prime asked for our SPRS score and evidence this week, who would answer, and with what?
2. Which of our vendors can see CUI, and have we checked their controls?
3. When did we last restore from backup, and how long did it take?

SEE IT BEFORE AN ASSESSOR DOES

Get your IT Risk Report.

Your security, compliance, and downtime exposure on your own inputs. Two minutes, no cost, no sales call.

Run the IT Risk Report

Sources: Verizon 2025 Data Breach Investigations Report; 32 CFR Part 170 (CMMC Program, effective Dec 16, 2024); DFARS CMMC acquisition rule (effective Nov 10, 2025); DFARS 252.204–7012; NIST SP 800–171 Rev. 2.

Readiness is not certification. This brief is not legal advice.