CyberEye

Measuring Risk. Prioritizing Action.

CMMC Readiness Checklist

Avoid a costly, unsuccessful certification assessment.
Use our checklist to ensure your organization is ready to initiate the C3PAO Assessment.

Not sure how to accomplish each step?
Enlist the help of our Certified Practitioners & Assessors (CCP/CCA) today!

		IN PROGRESS	NEEDS REVIEW	DONE
1	**CMMC Level & Data Types Defined** Review anticipated data types & DFAR Clauses	✔	✔	○
2	**Boundary Diagram with FCI/CUI Data Flow Depicted** Meets minimum *Scoping Requirements*	○	○	○
3	**Assets Inventoried** Includes all four (4) required asset types per *Scoping Requirements*	○	○	○
4	**Service Providers Identified** Cloud (CSP), External (ESP), Managed (MSP), Managed Security (MSSP)	○	○	○
5	**System Security Plan Complete** Includes *minimum content* and includes output of 1-4 (above)	○	○	○
6	**Policies & Procedures Documented** Policy and procedures exist for each security control	○	○	○
7	**Security Control Compliance Validated** Every assessment objective is addressed in the SSP or SRTM	○	○	○
8	**Service Provider Compliance Validated** Ensure *Customer Responsibility Matrix* is available for each SP	○	○	○
9	**Assessment Evidence & Artifacts Compiled** Ensure sufficient *evidence* is available for each security control	○	○	○
10	**No Unauthorized Assessment POA&M Entries Exist** Only controls listed in the 32CFR are authorized to be in the POA&M	○	○	○

PROCEED TO A C3PAO TO INITIATE CMMC ASSESSMENT PROCESS PHASES 1-4
Need to find one? We'll guide you to a few of our preferred, trusted C3PAOs

● Scoping   ● Documentation   ● Validation   ● Readiness

✉ info@cybereyesolutions.com   🌐 cybereyesolutions.com   🛡 Cyber AB Marketplace