FOR DEFENSE CONTRACTORS

CMMC Level 2 Readiness Planning Checklist

Bring clarity to scope, evidence, budget, and responsibility before you commit to a readiness program.

> Use this worksheet to organize a planning conversation. It is not a complete control assessment, an official SPRS submission, legal advice, or certification. Confirm current contract requirements and the applicable assessment path.

01 / DEFINE THE BOUNDARY

- ☐ **Confirm the requirement.** Identify the contract or solicitation, required CMMC level, assessment path, reporting obligations, and target milestone with your contracts lead.
- ☐ **Identify the information.** Document which workflows involve Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). Resolve uncertainty before selecting tools.
- ☐ **Map the flow.** Trace receipt, creation, access, sharing, storage, printing, backup, and disposal across users, devices, locations, and outside providers.
- ☐ **Inventory the environment.** List accounts, endpoints, servers, cloud services, applications, remote access, administrators, and supporting security services.
- ☐ **Compare boundary options.** Evaluate an enclave against the wider environment. Include administration, backups, integrations, and supporting systems before assuming savings.

Contract / workflow / planning owner

Systems and people expected inside the boundary

BUILD AN EVIDENCE-LED PLAN

Find the gaps. Assign the work.

02 / REVIEW SAFEGUARDS AND EVIDENCE

- [ ] **Choose the right baseline.** For the applicable CMMC Level 2 review, confirm the required NIST SP 800-171 revision and assessment procedures rather than mixing versions.
- [ ] **Review implementation.** Evaluate safeguards through interviews, examination, and testing as appropriate. A purchased license or written policy alone is not evidence that a safeguard operates.
- [ ] **Gather traceable evidence.** Identify relevant policies, configurations, access reviews, training records, logs, incident records, and recovery-test results. Record the owner and location of each artifact.
- [ ] **Maintain the SSP.** Describe the actual boundary, safeguards, dependencies, and responsibilities in the System Security Plan. Resolve differences between the document and operations.
- [ ] **Document and prioritize findings.** Assign an owner, target date, dependencies, and closure test to each remediation task. Confirm which gaps may be eligible for any conditional assessment path.

03 / MAKE CLOUD AND ACCESS DECISIONS

- [ ] **Evaluate the actual service.** Compare Microsoft 365 Commercial, GCC, GCC High, or other services against contract, data, access, and export-control needs. A cloud name alone does not establish compliance.
- [ ] **Confirm provider responsibilities.** Request relevant service documentation and agreements. Identify what your organization must configure, operate, monitor, retain, and prove.
- [ ] **Test the workflow.** Pilot identity, sharing, device access, backup, and recovery before a wider move. Record exceptions and acceptance criteria.

Highest-priority gap / accountable owner / next review date

TURN FINDINGS INTO A PRACTICAL NEXT STEP

Budget the program. Define ownership.

04 / PLAN DELIVERY AND ONGOING OPERATIONS

- ☐ **Separate budget lines.** Distinguish readiness consulting, remediation, licenses, ongoing security operations, internal staff time, and any independent assessment. Request a Custom Scope Quote.
- ☐ **Agree on responsibilities.** Name the people who own user support, monitoring, containment approvals, patching, backup checks, evidence, policy approval, and vendor escalation.
- ☐ **Preserve the agreed SLA.** Confirm coverage hours, response targets, exclusions, escalation, and customer responsibilities in the signed scope and existing SLA.
- ☐ **Validate before handoff.** Retest closed findings, review the evidence package, and confirm the authorized reporting process. A working score calculation is not an official submission.
- ☐ **Keep readiness current.** Schedule access reviews, evidence refreshes, recovery exercises, change reviews, and the affirmations or assessments required for your contract.

Next action / owner / target date

Make your next readiness decision with confidence.

Bring this worksheet, your contract requirements, and a high-level system inventory to a scoping conversation.

Request CMMC readiness support at rebnetik.com/cmmc-compliance

Official references

DoD CMMC program overview | dodcio.defense.gov/CMMC/About/

NIST SP 800-171 Revision 2 | Confirm the contract-required baseline.

Microsoft DFARS guidance | Review the specific service and its boundaries.

Prepared November 8, 2026. Program and service requirements may change. This checklist supports preparation and does not promise a particular assessment outcome.