

CMMC Level 1 Checklist

Readiness worksheet | Austin & Houston, Texas | Reviewed September 30, 2026

Start with scope, then verify implementation. Use this worksheet to organize preparation, evidence references, and corrective work. It summarizes the 15 FAR 52.204-21 safeguards; it is not the complete objective-level self-assessment or a certification.

Use the current official Level 1 Assessment Guide and mapped objectives for the actual assessment. Every requirement must be MET; Level 1 does not allow conditional status through an assessment POA&M.

Company / CAGE code(s):

Assessment scope / systems:

Assessment lead / Affirming Official:

Target assessment date / renewal owner:

- ☐ Confirm the required CMMC level and assessment type in the contract or subcontract.
- ☐ Identify where FCI is processed, stored, and transmitted, including external services.
- ☐ Document users, devices, system boundaries, and the systems covered by each CAGE.
- ☐ Assign an implementation owner and a reviewer for each safeguard.
- ☐ Collect evidence that reflects actual configurations and daily practices.

Status legend for pages 2-3: Ready = evidence prepared for objective-level assessment; Gap = correction needed; Review = unresolved. These are worksheet labels, not official MET determinations.

[BCS CMMC consulting services](#)

Safeguard review worksheet

FAR 52.204-21(b)(1) | Items 1-8

01 Restrict access to authorized users, processes, and devices. [FAR (b)(1)(i)]

Evidence ideas: Review account approvals, device records, service identities, and departed-user removal.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

02 Restrict users to permitted functions and transactions. [FAR (b)(1)(ii)]

Evidence ideas: Review role permissions and sample access tests for users with different duties.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

03 Control connections to external systems. [FAR (b)(1)(iii)]

Evidence ideas: Review approved remote access, outside devices, services, and connection restrictions.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

04 Control information on public systems. [FAR (b)(1)(iv)]

Evidence ideas: Review public website publishing approvals and checks for unintended disclosure.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

05 Identify users, processes, and devices. [FAR (b)(1)(v)]

Evidence ideas: Review inventories and identifiers, including service accounts and connected devices.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

06 Verify identities before granting access. [FAR (b)(1)(vi)]

Evidence ideas: Review authentication settings and tests for relevant users, devices, and processes.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

07 Sanitize or destroy FCI media before disposal or reuse. [FAR (b)(1)(vii)]

Evidence ideas: Review media handling procedures, sanitization records, and disposal receipts.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

08 Restrict physical access to authorized people. [FAR (b)(1)(viii)]

Evidence ideas: Review authorized-access lists and how rooms and equipment are secured.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

Evidence ideas are examples to help organize a review. Evaluate all mapped objectives and relevant assets; one record or product does not demonstrate the entire requirement.

Safeguard review worksheet

FAR 52.204-21(b)(1) | Items 9-15

09 Escort and monitor visitors; log access; manage access devices. [FAR (b)(1)(ix)]

Evidence ideas: Review visitor procedures, access logs, and key or badge issuance and revocation.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

10 Protect communications at external and key internal boundaries. [FAR (b)(1)(x)]

Evidence ideas: Review network diagrams, boundary configurations, rules, and verification records.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

11 Separate public-facing components from internal networks. [FAR (b)(1)(xi)]

Evidence ideas: Review public-facing systems and physical or logical separation and access tests.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

12 Identify, report, and correct flaws promptly. [FAR (b)(1)(xii)]

Evidence ideas: Review patching records, reported flaws, remediation tickets, and follow-up checks.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

13 Provide malicious-code protection where appropriate. [FAR (b)(1)(xiii)]

Evidence ideas: Review protection deployment, coverage, configurations, and alerts.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

14 Keep malicious-code protection updated. [FAR (b)(1)(xiv)]

Evidence ideas: Review update settings, current versions, and recent update or failure records.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

15 Scan systems periodically and external files in real time. [FAR (b)(1)(xv)]

Evidence ideas: Review scan schedules, results, real-time settings, and handling of external files.

Status: Ready / Gap / Review Owner: _____

Evidence reference / action: _____

Evidence ideas are examples to help organize a review. Evaluate all mapped objectives and relevant assets; one record or product does not demonstrate the entire requirement.

Assessment & submission plan

Close gaps, complete assessment, affirm, and maintain compliance

- ▣ Resolve assessment gaps and verify implementation against every mapped objective.
- ▣ Confirm the assessment date, scope, compliance result, and included CAGE codes.
- ▣ Confirm PIEE access and an approved SPRS Cyber Vendor User role for the right CAGE.
- ▣ Enter the Level 1 assessment through SPRS Cyber Reports and CMMC Assessments.
- ▣ Have the authorized company Affirming Official review and complete the affirmation.
- ▣ Verify Final Level 1 Self-Assessment status; save the CMMC UID and record details.
- ▣ Schedule the next annual self-assessment, results submission, and affirmation.
- ▣ Retain assessment evidence artifacts for six years from the CMMC Status Date.

Priority gap / action:

Owner / due date / reviewer:

Evidence location / CMMC UID:

Need help turning findings into completed work? BCS offers scope reviews, gap reviews, technical remediation, evidence organization, and self-assessment preparation. Your authorized company officials retain responsibility for reporting and affirmation.

Official FAR safeguards: acquisition.gov/far/52.204-21

Official Level 1 assessment guidance

SPRS guides and tutorials: sprs.csd.disa.mil/cmmc.htm

CMMC program rule: 32 CFR Part 170 (170.15 and 170.22)

BCS preparation worksheet. Confirm contract requirements and use current official guidance. No CMMC outcome is guaranteed by completing this worksheet.