

CMMC Level 1 Self-Assessment Checklist

The 15 FAR 52.204-21 basic safeguarding requirements, grouped by CMMC family. Hawkcrest Cyber · hawkcrestcyber.com

At a glance

- **Applies to:** DoD contractors and subcontractors handling Federal Contract Information (FCI), not CUI, on their own systems (32 CFR 170.3, 170.23).
- **Frequency:** self-assessment every year, results entered in SPRS; Affirming Official affirms after each assessment and annually (32 CFR 170.15, 170.22).
- **Deadline:** assessment and affirmation must be in SPRS before award of a contract or subcontract requiring Level 1 (32 CFR 170.15(b)). SPRS marks a Final Level 1 status expired after 1 year.
- **Pass/fail:** all 15 must be MET; no POA&Ms at Level 1 (32 CFR 170.24(c)(1)). Keep evidence 6 years (32 CFR 170.15(c)(2)).

- ☐ **0. Scope defined:** every system, person, facility, and external service provider that processes, stores, or transmits FCI is listed (32 CFR 170.19(b)).

Access Control (AC)

- ☐ **1. AC.L1-b.1.i** "Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)."
Only people, programs, and devices you've approved get in.
Evidence: a current list of user accounts and company devices, with no leftover accounts for people who've left.
- ☐ **2. AC.L1-b.1.ii** "Limit information system access to the types of transactions and functions that authorized users are permitted to execute."
People can only do what their job needs. Day-to-day accounts aren't admin accounts.
Evidence: role or group lists, and a short list of who has admin rights.
- ☐ **3. AC.L1-b.1.iii** "Verify and control/limit connections to and use of external information systems."
Decide whether personal phones, home PCs, personal email, or outside file-sharing sites can touch FCI, and enforce it.
Evidence: a written rule plus the settings that back it up.
- ☐ **4. AC.L1-b.1.iv** "Control information posted or processed on publicly accessible information systems."
Make sure FCI doesn't end up on your website, social media, or a public share link.
Evidence: who's allowed to post publicly and how posts get reviewed.

Identification and Authentication (IA)

- ☐ **5. IA.L1-b.1.v** "Identify information system users, processes acting on behalf of users, or devices."
Everyone gets their own named account. No shared "shop" or "front desk" login.
Evidence: the user and device list.
- ☐ **6. IA.L1-b.1.vi** "Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems."
Prove who you are before you get in. Passwords at minimum, and change default passwords on new gear.
Evidence: your password settings and sign-in policy.

Media Protection (MP)

- ☐ **7. MP.L1-b.1.vii** "Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse."
Wipe or shred drives, USB sticks, and paper before they're tossed, sold, or handed down.
Evidence: a disposal process and wipe or destruction records.

Physical Protection (PE)

- ☐ **8. PE.L1-b.1.viii** “Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.”
Lock the server closet and the office. Only the right people have keys or badges.
Evidence: a key or badge list.
- ☐ **9. PE.L1-b.1.ix** “Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.”
Three things here: escort visitors, keep a visitor log, and track keys, fobs, and badges (and get them back when people leave).
Evidence: the visitor log and your key/badge tracking.

System and Communications Protection (SC)

- ☐ **10. SC.L1-b.1.x** “Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.”
Have a properly configured firewall between your network and the internet.
Evidence: firewall make and model, and its rules.
- ☐ **11. SC.L1-b.1.xi** “Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.”
Anything the public can reach (a self-hosted web server, guest Wi-Fi) sits on its own network, apart from your business systems.
Evidence: a simple network diagram. If you truly have no publicly accessible system components in scope, this may be N/A: 32 CFR 170.24(b)(3) gives that example for the matching Level 2 control SC.L2-3.13.5 (same NIST 3.13.5 requirement), and N/A counts as MET. Document why.

System and Information Integrity (SI)

- ☐ **12. SI.L1-b.1.xii** “Identify, report, and correct information and information system flaws in a timely manner.”
Keep up with patches for Windows, Mac, apps, firewalls, and other gear.
Evidence: patch settings and update history.
- ☐ **13. SI.L1-b.1.xiii** “Provide protection from malicious code at appropriate locations within organizational information systems.”
Antivirus or endpoint protection on your computers, and email filtering.
Evidence: a console view showing which devices are protected.
- ☐ **14. SI.L1-b.1.xiv** “Update malicious code protection mechanisms when new releases are available.”
That protection updates itself automatically.
Evidence: the update setting and last-updated dates.
- ☐ **15. SI.L1-b.1.xv** “Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.”
Scheduled scans plus real-time scanning of downloads, email attachments, and USB files.
Evidence: scan schedule and real-time protection settings.

Assessment date: _____ Assessed by: _____ Affirming Official: _____
SPRS entry/affirmation date: _____

Requirement text quoted from FAR 52.204-21(b)(1) (ecfr.gov). Assess using NIST SP 800-171A objectives per 32 CFR 170.15(c)(1). Checked against official sources Oct. 11, 2026; CMMC is under DoD review, so confirm current status at dodcio.defense.gov/CMMC. General information, not legal advice.