Explore the CMMC Level 1 Evidence Guide

A practical, contractor-friendly example pack showing exactly what auditors expect to see for each Level 1 practice

CMMC Level 1 includes **17 practices** across **6 domains**, all aligned directly to the safeguarding requirements in FAR 52.204-21. This guide shows **what auditors expect**, **what counts as acceptable evidence**, and **simple examples that small contractors can immediately recognize** in their own environment.

---

1. ACCESS CONTROL (AC)

AC.L1-3.1.1 — Authorized Access Control

What auditors look for:

- Proof that only authorized users can access systems processing FCI
- Evidence that accounts are created intentionally, not automatically

Acceptable evidence examples:

- User access list showing active accounts only
- Screenshot of account creation approval workflow
- MSP onboarding/offboarding procedure
- Email or ticket showing supervisor approval

AC.L1-3.1.2 — Limit Access to Authorized Users (Least Privilege)

What auditors look for:

- Users only have the access they *need* to do their job

Acceptable evidence examples:

- Role-based access matrix
- Screenshot showing restricted folder permissions
- M365/Google Workspace role assignments
- Ticket showing access change approval

AC.L1-3.1.20 — External Connections Controlled

What auditors look for:

- How remote access or integrations are approved and limited

Acceptable evidence examples:

- Screenshot showing MFA enforced for remote access
- VPN configuration with restricted user list
- List of allowed third-party integrations / API connections
- Firewall rule set showing limited inbound access

---

2. IDENTIFICATION & AUTHENTICATION (IA)

IA.L1-3.5.1 — Identify Users Uniquely (No Shared Logins)

What auditors look for:

- Proof that every human has a unique username

Acceptable evidence examples:

- AD / Entra ID user list
- Policy forbidding shared accounts
- Screenshot of login settings

IA.L1-3.5.2 — Authenticate Users (Passwords / MFA)

What auditors look for:

- MFA enforced wherever FCI is accessed
- Minimum password configuration

Acceptable evidence examples:

- Screenshot of MFA enforcement in M365/Google
- Password policy screenshot (length, lockout, complexity)
- Evidence of MFA enrollment for staff

3. MEDIA PROTECTION (MP)

MP.L1-3.8.3 — Sanitization of FCI Before Disposal

What auditors look for:

- A repeatable process for wiping or destroying media containing FCI

Acceptable evidence examples:

- Asset disposal log
- Certificate of destruction for hardware
- Screenshot of laptop wipe workflow from RMM
- Policy/procedure for media sanitization

---

4. PHYSICAL PROTECTION (PE)

PE.L1-3.10.1 — Limit Physical Access to Systems with FCI

What auditors look for:

- Businesses have *basic* controls: locked door, restricted room, badge, etc.

Acceptable evidence examples:

- Photos of locked server/network closets
- Visitor log template
- Office access policy
- Lease agreement showing secure office environment

PE.L1-3.10.3 — Escort Visitors & Monitor Access

What auditors look for:

- Visitors are not roaming freely where FCI may be present

Acceptable evidence examples:

- Visitor check-in sheet
- Policy requiring escorts
- Sign posted at front desk

5. SYSTEM & COMMUNICATIONS PROTECTION (SC)

SC.L1-3.13.1 — Boundary Protection (Firewalls, Filters, TLS)

What auditors look for:

- Proof that external connections are filtered and protected

Acceptable evidence examples:

- Firewall screenshot showing rules
- Email security settings (anti-spam, anti-phish)
- Certificate showing TLS in use
- RMM report showing firewall enabled on endpoints

SC.L1-3.13.5 — Limit Public Information Posting

What auditors look for:

- Contractors do *not* post FCI on public websites or portals

Acceptable evidence examples:

- Policy stating FCI cannot be public
- Training slides reminding staff
- Verification that public website contains no sensitive detail

---

6. SYSTEM & INFORMATION INTEGRITY (SI)

SI.L1-3.14.1 — Identify, Report, and Correct Flaws (Patching)

What auditors look for:

- Systems receive updates on a predictable schedule

Acceptable evidence examples:

- RMM patching report from last 30 days
- Screenshot of auto-update settings for OS/software
- Ticket showing emergency patch process

SI.L1-3.14.2 — Protect Against Malicious Code (AV/EDR)

What auditors look for:

- Anti-malware is installed, running, and updating

Acceptable evidence examples:

- Screenshot of AV/EDR dashboard
- Monthly health report
- Policy requiring AV on all devices
- Quarantine log sample

SI.L1-3.14.4 — Conduct Regular & Real-Time Scans

What auditors look for:

- Malware scanning is happening automatically

Acceptable evidence examples:

- Endpoint scan schedule screenshot
- AV dashboard showing recurring scans
- RMM-generated endpoint compliance report

📄 **Bonus: Auditor-Friendly "Evidence Pack" Template**

Your evidence pack for each Level 1 practice should include:

1. **Policy/Procedure:** 1–2 pages max
2. **Technical Evidence:** Screenshots or reports
3. **Administrative Evidence:** Tickets, approvals, logs
4. **Attestation:** "This is how we do it today" summary

If you want, I can generate all 17 evidence pack templates pre-filled for your use in assessments.