FIRSTCALL FEDERAL

CMMC EVIDENCE STARTER KIT

Know exactly what to show your C3PAO before they walk in the door.

www.firstcallfederal.com

READ THIS FIRST

If you can't prove it, it doesn't count.
Most DoD contractors have policies, tools, and good intentions. They fail CMMC because they cannot show clear, consistent evidence that controls are working.

This kit gives you three things:

- Pass/Fail evidence examples for high-friction areas
- A 12-point "fail early" checklist you can use in a 30–45 minute internal review
- A practical guide to prepare staff for audit interviews without scripts or fear

Use this as a working document: mark it up, assign owners, and bring your questions to your next call with our team.

How to use this kit

Start with the checklist.
Run through the 12 questions and be brutally honest. If you can't find an artifact in 5 minutes, mark it as "No."

Compare your evidence to the examples.
For each area, pull a real sample from your environment and see whether it looks more like the "Pass" or "Fail" example.

Capture your action items.
For every gap, write down: owner, target date, and what evidence will look like when it's fixed.

Decide your next move.

- Mostly "Pass": you may be ready to plan a formal readiness review or assessment.
- Mostly "Fail": you're early; this is the best time to get guidance before spending more.

Use this kit with your MSP or internal IT team. It is designed to be collaborative, not accusatory.

Pass/Fail Examples - Access Control

Access Control: Who can see what And how you PROVE it.

FAIL

User Access List

- Outdated spreadsheet from last year; no clear mapping to in-scope systems.
- Admins only have privileged accounts; no disabled accounts for departed staff.

PASS

User Access List

- Current export from identity system (e.g., AD, Azure AD) filtered to in-scope systems.
- Clear role descriptions, separated privileged accounts, and last login dates.

What your assessor is thinking:
“Can this organization quickly show who has access to CUI systems and why?”

FAIL

Access Request & Approval

- Verbal approvals; no ticket or documented workflow.
- No record of who approved elevated access.

PASS

Access Request & Approval

- Tickets or forms showing who requested access, who approved it, and when it was granted.
- Evidence that access changes are tied to role changes or onboarding/offboarding.

FAIL

Periodic Access Review

- “We review access sometimes” but no meeting notes, sign-offs, or tracked changes.

PASS

Periodic Access Review

- Quarterly or semiannual review records: attendee list, date, systems reviewed, and decisions taken.

If you cannot show at least one full access review cycle with decisions and follow-up, expect tough questions.

Examples - Auditable Logs and CUI Handling

Logging: Proving you see and respond to security-relevant events.

FAIL

Fragmented Logging

- Logs scattered across servers, appliances, and tools; no central view.
- No clear retention period or time sync.

PASS

Fragmented Logging

- Screenshot from SIEM or log system showing in-scope systems sending logs.
- Documented retention policy and NTP/time sync configuration.

FAIL

Log Review & Alerts

- “Our tool alerts us,” but no evidence of actual reviews or investigations.

PASS

Log Review & Alerts

- Tickets, emails, or SIEM reports that show periodic log review and response to alerts.

CUI Handling: Where critical information lives and how you protect it.

FAIL

CUI Data Map

- No current documentation of where CUI is stored, processed, or transmitted.

PASS

CUI Data Map

- Diagram or document listing CUI repositories (file shares, apps, cloud services) plus access controls and encryption.

FAIL

Labeling & Segmentation

- CUI mixed with non-CUI content; same shares and permissions; no clear labels.

PASS

Labeling & Segmentation

- Labeled locations, separated by access controls; screenshots of permissions and encryption settings.

Pass/Fail Examples - Training Records

Training: Showing your people know what to do.

FAIL

Annual Security Awareness

- “We told people in a meeting” with no attendance records or completion list.

FAIL

Role-Based Training

- Admins and high-privilege users receive the same training as everyone else.

PASS

Annual Security Awareness

- LMS export or signed roster showing who completed training and when.

PASS

Role-Based Training

- Additional modules or sessions for admins, help desk, and developers, with separate completion records.

“Fail Early” CMMC Checklist

If you can’t provide these 12 items, you will likely fail early.

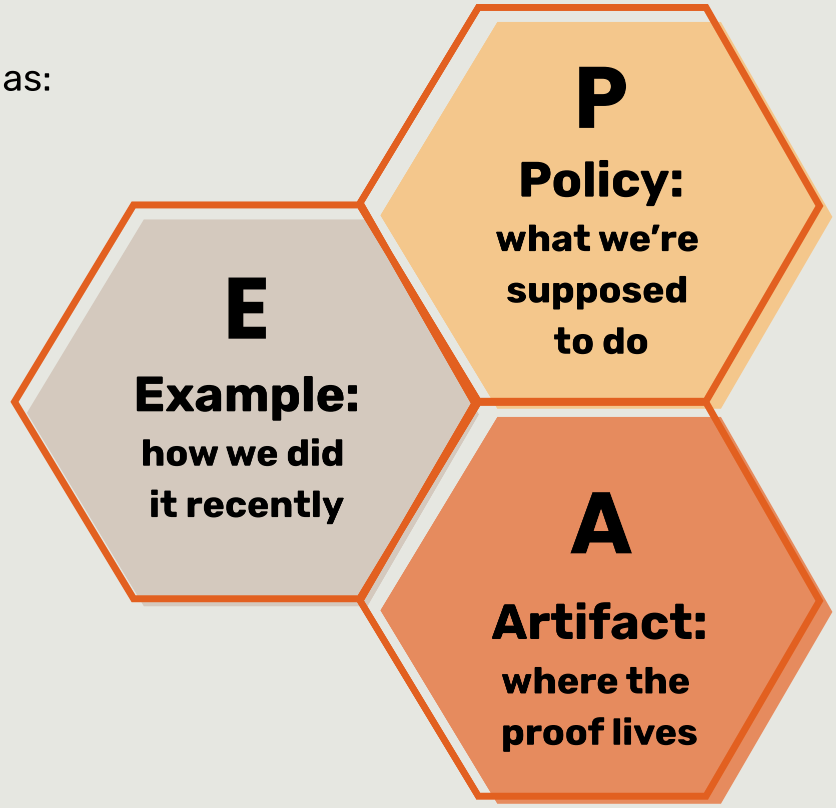
	Yes	No	Own
1. Current signed SSP aligned to NIST 800-171 / CMMC 2.0 scope	□	□	□
2. Network and data flow diagrams showing CUI and boundary	□	□	□
3. Documented asset inventory of in-scope systems and services	□	□	□
4. Access control records: user listings, approvals, reviews	□	□	□
5. MFA evidence for remote and privileged access	□	□	□
6. Central log collection and retention evidence	□	□	□
7. Incident response plan plus at least one test or tabletop	□	□	□
8. Backup and recovery evidence for CUI systems	□	□	□
9. Encryption configuration documentation (at rest / in transit)	□	□	□
10. Security awareness and role-based training records	□	□	□
11. POA&M with owners and realistic dates	□	□	□
12. Policy & procedure review/approval history for 12–18 months	□	□	□

If you marked ‘No’ on 3 or more items, consider a structured readiness review before scheduling an assessment.

Preparing Your Team for CMMC Interviews

Assessors are not trying to trick your staff; they are trying to understand whether your processes really operate the way your documents claim.

The PEA Answer Model
Ask staff to structure answers as:



P

Policy: what we're supposed to do

E

Example: how we did it recently

A

Artifact: where the proof lives

Example:
When you request access for a new engineer, how does that work?

Policy: Our policy requires a ticket and manager approval.

Example: Last month we onboarded Jane; here's the ticket we used.

Artifact: That ticket lives in System X; the approval is in the comments.

TOP 7 TOPICS TO REHEARSE

1. **How they request / change / remove access**
2. **How they report suspicious emails or incidents**
3. **How they handle CUI (storage, sharing, disposal)**
4. **How they use personal or mobile devices**
5. **How they connect remotely and use MFA**
6. **What training they receive and how often**
7. **Who they escalate problems to**

IMPORTANT REMINDERS

Do:

- Answer from your real experience
- Say "I'm not sure; here's who would know" when appropriate

Don't:

- Guess or invent processes you don't actually follow
- Panic if you need to look something up—assessors expect that

WHAT TO DO AFTER YOU USE THIS KIT...

- **If you scored strong on the checklist:** schedule a targeted readiness review to validate your evidence.
- **If you found major gaps:** get a prioritized remediation roadmap before investing in tools or a formal assessment.

Ready for a CMMC Evidence Review?

Share your completed checklist and example artifacts, and a FirstCall Federal advisor will give you specific feedback on where you're ready and where you're at risk.

Schedule your evidence review