DEFENSE CONTRACTORS

What a CMMC Assessment Actually Asks You to Show

Most CMMC effort goes into deciding what to implement. Assessments turn on something narrower — whether you can produce evidence that it runs. A guide to the difference.

Cyberneza LLC | Veteran-Owned | Orlando, FL
cyberneza.com | info@cyberneza.com

Want a second opinion on your scope?
Start a conversation:
cyberneza.com/contact

The distinction that decides assessments

A control can be genuinely selected, correctly designed, accurately written into your System Security Plan, and still fail an assessment. Not because anyone lied — because nothing in the environment performs it, and the assessment asks for proof that it does.

Assessors work from a simple posture: if it is not written down, it does not exist. But the converse trips more programmes. Written down is not the same as happening, and the second question is the one a document review cannot answer and an interview can.

Three states a control can be in

1. Absent. Nothing exists. Honest, visible, and the easiest of the three to fix.
2. Documented. A policy describes it. Nothing performs it, nobody reviews it, and no record accumulates. This is where self-assessments overstate, because from the inside it feels done.
3. Operating. It runs, it produces records, and somebody looks at them. Only this state survives an assessment.

The gap between the second and third state is where most remediation time actually goes, and it is almost never discovered early enough.

Scope is the decision that sets the cost

Everything else is downstream of where CUI lives and travels. A minimised, clearly defined boundary — an enclave, a separated system — is dramatically cheaper to assess than a corporate network that grew organically. This is the single highest-leverage decision in a CMMC programme, and it is made early, when it is least obvious that it matters.

What an assessor will press on

- Where CUI enters, is created, stored, transmitted, and destroyed — as a diagram you can walk through
- Why the boundary is drawn where it is, defended rather than asserted
- What connects to the boundary and how that connection is controlled
- Every device that can store or process CUI, including laptops and mobile endpoints
- Whether anything outside the boundary can reach inside it

The flat-network trap

Without segmentation, scope expands to fill the environment. One unmanaged workstation sharing a flat network with a CUI system can pull the whole estate into assessment. Segmentation is not a technical nicety here; it is the difference between a contained assessment and an unbounded one.

What evidence looks like, by family

Some requirement families are satisfied by configuration you can screenshot. Others describe continuous activity, and for those the evidence is a record accumulated over time. Those are the ones worth checking early, because they cannot be produced retroactively.

Audit & Accountability (AU)

- Logs centralized off the systems that generate them, and retained for the required period
- Evidence that someone reviews them — review records, not just collection
- The ability to reconstruct what happened during a specific past event

System & Information Integrity (SI)

- Endpoint monitoring that is deployed, current, and actually reporting
- Records of alerts raised, investigated, and closed
- Monitoring of inbound and outbound traffic, not only host-level protection

Incident Response (IR)

- A plan, and evidence it has been exercised — a tabletop with a dated record
- Detection capability that would actually feed the plan
- Records of real incidents handled, however minor

Identification & Authentication (IA)

- Multi-factor authentication deployed universally across in-scope remote and privileged access
- Evidence of coverage, including the accounts and systems that are exceptions and why
- FIPS-validated cryptography where the requirement calls for it

Awareness & Training (AT)

- Completion records per person, dated
- Role-specific content where roles differ
- Evidence that people outside IT understand the policies that apply to them

The interview is part of the assessment

Assessors do not only examine systems. They talk to people — help desk staff, system administrators, HR, management — to establish whether policies are understood and practised rather than merely published.

This produces a failure mode worth internalising: a policy known only to the IT team is not considered implemented. If the person who handles new starters cannot describe the onboarding security steps, the control is not operating regardless of what the procedure says.

Preparing people, not just systems

- Key personnel must be available throughout the assessment. Unavailability stalls it, and a stalled assessment is a failing one.
- Walk the people who will be interviewed through the questions they are likely to face.
- Do not script them. Assessors can tell, and a rehearsed answer that does not match practice is worse than an honest one that does.

The C3PAO cannot help you

Once the assessment begins, the assessing organization evaluates and reports — it cannot advise on fixes. Every remediation has to be complete beforehand. If you want help getting there, that is a separate engagement with a separate party, arranged in advance.

Five ways good programmes still go wrong

1. Treating it as a project with a deadline. Readiness is commonly a 6–18 month effort. Starting when a contract requires certification means starting late.
2. Buying tooling and considering the control closed. A firewall, EDR platform or logging system that is installed but untuned and unwatched produces no evidence and satisfies no requirement.
3. Forgetting that CMMC is not only technical. Visitor logs, badge access, server room security, background checks and termination procedures are assessed alongside the technical safeguards.
4. Ignoring the supply chain. You are accountable for subcontractors and vendors that touch your CUI, and assessors will ask how you vet, contractually bind and monitor them.
5. Chasing a perfect score before starting. Gaps tracked honestly on a POA&M are a normal part of the process; cancelling an assessment over a handful of them usually costs more than it saves.

What to do in the next thirty days

1. Draw the CUI data flow. If it cannot be drawn, the boundary is not yet defined, and nothing downstream is reliable.
2. Pick one security-relevant event from last month and trace who reviewed it and when. If the answer is nobody, your audit and accountability practices are documented rather than operating.
3. List every device that can touch CUI, including personal and mobile ones, and check each is encrypted and managed.
4. Read your SSP as if you were an assessor looking for a claim the environment does not support. There is usually at least one.
5. Identify which requirements need something running continuously, and decide who runs it.

A second opinion before the assessment, not during it

Cyberneza scopes the CUI boundary, assesses current state against the practices, and is explicit about which requirements are documented rather than operating. Fixed-fee assessment, credited toward later work.

cyberneza.com/contact

Sources and scope

This guide draws on Cyberneza's assessment and architecture experience, and on published partner material from Huntress — specifically its CMMC Level 2 assessment one-pagers on common pitfalls and preparation. Cyberneza is an authorized Huntress reseller.

It is deliberately about evidence practice rather than certification mechanics. The CMMC rollout schedule has changed more than once, and material written against a particular phase dates quickly; the evidence expectations described here are stable across those changes. For current programme status, see cyberneza.com/blog.

Nothing here is a determination of compliance. Whether a practice is met is decided by your self-assessment or your C3PAO, and any action should be tailored to your environment.