GUIDE

Redspin

Why Organizations Fail CMMC Recertification

(After Passing the First Time)

Real patterns C3PAOs are seeing, and how to avoid them

Recertification is not a repeat of certification

A lot of organizations walk into recertification assuming it will feel like a lighter version of what they already did. It's not. Initial certification proves you implemented the controls. Recertification proves you've been operating them correctly over time. That's where things start to break.

At Redspin, we've seen this play out across environments of all sizes, organizations that were fully compliant at certification, but three years later, small gaps have compounded into real risk. Not because they didn't care. Because maintaining CMMC is fundamentally different than achieving it. What follows are the most common patterns we're seeing in recertification failures and what's actually behind them.

1. The SSP Looks Right... Until It Doesn't Match Reality

The System Security Plan (SSP) is often strong at certification. It's reviewed, approved, aligned. Then the environment evolves. Cloud configurations change. New tools are introduced. M365 settings shift. Data flows expand. Systems are added or retired. But the SSP doesn't keep up.

What assessors see at recertification is not a bad SSP, it's an outdated one. A document that reflects what the environment used to be, not what it is today. This is one of the most common reasons recertifications are delayed or fail.

Why it happens:
Teams treat the SSP as an artifact created for the assessment, not as a living system description that needs to evolve alongside the environment.

What recertification tests:
Alignment between documentation and reality, not just whether the document exists.

2. “We Do This” Isn’t Enough Without Proof Over Time

At certification, organizations can often demonstrate controls with a combination of interviews and recent evidence. At recertification, that bar is higher.

Assessors are looking for consistency over time, not snapshots. We routinely see:

- Log reviews being performed, but not retained
- Training completed once, but not repeated
- Incident response tested once, then never revisited
- Vulnerability scans run, but no historical record maintained

The control may exist. The activity may even be happening.
But without evidence that shows it’s been happening continuously, it doesn’t hold up.

Why it happens:
Organizations focus on “being compliant” instead of building repeatable, documented operational cadence.

What recertification tests:
Whether your controls are part of your day-to-day operations, not just your assessment preparation.

3. Annual Affirmations Become a Checkbox Exercise

Between certification and recertification, organizations are required to annually affirm their compliance. In practice, this is often treated as administrative. Affirmations get submitted without:

- Re-validating control implementation
- Assessing changes to the environment
- Reviewing supporting evidence
- Fully briefing the Affirming Official on risk

This is a problem. Post-Final Rule, affirmations carry real weight, and real risk.
A careless affirmation isn’t just a process gap. It can introduce False Claims Act exposure.

Why it happens:
The process feels routine, so the rigor drops.

What recertification tests:
Whether your organization actually validated its compliance year over year, or just attested to it.

4. The Environment Changes, But the Scope Doesn’t

Over a three year period, environments don’t stay static, they:

- Take on new contracts involving CUI
- Expand cloud usage
- Introduce new tools and services
- Add subcontractors or external partners
- Enable new remote access paths

But scope doesn’t always get revisited.

At recertification, this shows up clearly:

- CUI stored outside the defined enclave
- Systems interacting with CUI that aren't in scope
- External service providers introduced without proper validation
- Boundary definitions that no longer reflect actual data flow

This is one of the most consistently cited failure points at Level 2.

Why it happens:
Scope is treated as a one-time exercise instead of something that needs periodic re-evaluation.

What recertification tests:
Whether your defined boundary still accurately represents where CUI lives and flows.

5. ESP Compliance Drifts Without Anyone Noticing

External Service Providers (ESPs) are often a key part of an organization's compliance strategy. At certification, everything is aligned:

- FedRAMP Moderate (or equivalent) is verified
- Shared Responsibility Matrices are documented
- SSP reflects inherited controls

Then things change. Licensing tiers shift. New services are introduced. Temporary tools become permanent. Vendors evolve. And the assumption becomes "If the vendor is compliant, we're covered." That's not how assessors view it. Organizations remain responsible for inherited controls—and must prove:

- Current compliance status of the ESP
- Clear shared responsibility
- Accurate reflection in the SSP

Why it happens:
Vendor environments change quietly, and internal teams don't always reassess the impact.

What recertification tests:
Whether you've actively managed your reliance on ESPs—or just assumed it stayed valid.

6. Configuration Management Quietly Breaks Down

Configuration management is one of those areas that looks strong on paper. Policies exist. Procedures are defined. Baselines are documented. But over time:

- Changes aren't consistently tracked
- Approvals become informal
- Patch cycles slip
- Privileged access expands without review

This is where assessors often find issues during technical validation, not because controls don't exist, but because they aren't being enforced.

Why it happens:
Operational pressure overrides process discipline.

What recertification tests:
Whether your technical environment still aligns with your defined security baseline.

7. Turnover Erodes Institutional Knowledge

This one is quieter, but just as impactful. Over three years, people change roles, leave the organization, or shift responsibilities. When that happens:

- Control ownership becomes unclear
- New team members aren't trained on CMMC responsibilities
- Role-based training isn't repeated
- Key processes (like IR or logging review) lose consistency
-

At recertification, this shows up as gaps in execution, not intent.

Why it happens:
Organizations underestimate how much compliance depends on people, not just systems.

What recertification tests:
Whether your program is resilient to change—or dependent on specific individuals.

What Recertification Actually Validates

Recertification is not about whether you had a compliant environment. It's about whether you've been able to sustain it. Assessors are looking for:

- Alignment between documentation and reality
- Evidence of consistent operation over time
- Clear ownership and accountability
- A defined scope that reflects actual data flow
- Controls that are not just implemented, but also maintained

This is why recertification often feels harder. Because it is.

Don't Wait for Recertification to Surface the Gaps

Most organizations don't fail because they lack controls. They fail because things drift, slowly, quietly, and over time.

The good news is, these issues are predictable. And if they're predictable, they're preventable.

You passed once.
Now prove you can sustain.
Validate your readiness before recertification does.

WHY REDSPIN

- One of the first Authorized C3PAOs, with one of the largest in-house teams of certified assessors
- Proven at scale, having conducted a significant portion of all CMMC Level 2 assessments to date
- Real-world experience across readiness, certification, and ongoing compliance
- CAP aligned assessment approach focused on validation, not “check-the-box” assessments
- Purpose-built cloud and managed compliance solutions designed to simplify scope and accelerate CMMC
- Clear separation between assessment and managed services to maintain independence and trust
- Deep involvement in the CMMC ecosystem since day one, with insight into how requirements are actually being applied

Redspin, the federal division of Clearwater, is one of the first Authorized CMMC 3rd-Party Assessment Organizations (C3PAOs) and is the most experienced team of assessors in the ecosystem. As a trusted partner to the Defense Industrial Base, Redspin helps organizations prepare for, achieve, and sustain CMMC through training, assessments, readiness consulting, managed compliance, and secure cloud services.

From building your program to proving it—and maintaining it—Redspin protects the DIB as a service.

Redspin

40 Burton Hills Blvd
Suite 410
Nashville, TN 37215

info@redspin.com
www.redspin.com
contact us