COALFIRE FEDERAL

The CMMC Between-Certification Playbook

How to Sustain CMMC Level 2 Certification, Reduce Compliance Risk, and Stay Assessment-Ready Across the Full Three-Year Cycle

The Certification Is Behind You. The Hard Part Isn't.

Picture this: A defense contractor passed their CMMC Level 2 assessment two-and-a-half years ago. Since then, they've onboarded new staff, migrated a system, and reorganized two departments. Nobody updated the System Security Plan. Evidence collection has been inconsistent. The person who owned access reviews left a year ago.

Recertification is now six months away. What looked like a solved problem is about to become an expensive emergency.

This scenario is not an exception across the Defense Industrial Base. It is the rule, and it is entirely preventable.

60%+

of contractors rate the difficulty of CMMC compliance a 7/10 or higher*

The Three Realities of Ongoing CMMC Compliance

CMMC Level 2 certification is not a point-in-time event. Achieving certification is a milestone, but it is not the finish line.

Certification marks the beginning of a new operating model, one built on continuous accountability, repeatable evidence, and ongoing control performance. Passing a Level 2 assessment proves that your organization met the standard at a specific point in time. Maintaining the certification requires proving that those controls continue to function long after the assessor leaves.

Organizations across the Defense Industrial Base are discovering the same reality: compliance does not stay static. Systems change. Employees leave. Evidence gets lost. Without a deliberate strategy between assessments, readiness decays faster than most teams expect.

There are three realities of ongoing compliance every contractor must plan for:

Controls must be maintained continuously

Security practices aligned with NIST SP 800-171 cannot pause after CMMC certification. Access reviews, incident response testing, vulnerability management, training, and configuration management must continue consistently, not just before an audit.

Evidence must be reproducible

Assessors need proof, not assumptions. If evidence cannot be located, repeated, or defended, the control may effectively fail.

Annual affirmation is enforceable, not symbolic

Annual affirmations are formal attestations to the Department of War, not administrative checkboxes. Leadership is signing off that required controls remain implemented and effective.

*https://info.cybersheath.com/eBook-Third-Annual-Merrill-Research-Report

The CMMC Certification Lifecycle

CMMC follows a structured, three-year certification cycle. Understanding where your organization sits within this lifecycle determines what actions are required right now.

Pre-Assessment Readiness

Before initial certification, organizations implement required controls, remediate gaps, validate evidence, and establish internal ownership. This phase receives significant focus because it leads directly to the C3PAO assessment. Many organizations invest heavily here and then under-invest in what comes next.

Year 0

Initial Certification Assessment

Your Certified Third-Party Assessment Organization (C3PAO) evaluates whether your environment meets CMMC Level 2 requirements. If successful, certification is granted. But the responsibility does not stop there.

Years 1 and 2

Annual Affirmation and Self-Assessment

Between formal assessments, organizations must maintain control effectiveness and submit annual affirmations supported by internal validation and self-assessment activities. This is when many compliance programs weaken, typically from the absence of deliberate structure.

Year 3

Recertification

Recertification is not a restart; it is a validation that your organization sustained compliance over time. Teams that maintained readiness move through this phase predictably. Teams that allowed drift often face expensive remediation and delayed contract eligibility.

CMMC Level 2 Lifecycle Timeline

What "Between Certification" Means

The time between initial certification and Year 3 recertification is not a compliance pause. It is the period during which certification is either preserved or lost, and most organizations do not find out which until it is too late to fix it.

During this period, organizations are accountable for:

- Continuous control execution
- Ongoing evidence generation and retention
- Internal validation of control effectiveness
- Managing the risk of compliance drift

Over time, even well-prepared organizations experience compliance decay, where controls weaken, evidence gaps emerge, and alignment erodes due to system changes, personnel turnover, and shifting priorities.

Without deliberate structure between certifications, readiness degrades faster than most organizations expect.

Annual Affirmation and Self-Assessment: What Leadership Is Actually Signing

The annual affirmation is often misunderstood as a paperwork exercise. In practice, it is one of the highest-risk moments in the certification lifecycle, particularly for the compliance officers and executives who sign it.

It is a formal attestation to the Department of War

Leadership is affirming that the organization continues to meet required CMMC obligations. This attestation is submitted to the Supplier Performance Risk System (SPRS) and is a formal representation of compliance posture to the Department of War. An inaccurate or unsupported affirmation creates legal, contractual, and operational risk.

The accountability falls on leadership

Executives are not expected to personally manage every control, but they are responsible for ensuring the organization can defend the attestation they are signing. Confidence in that signature requires organizational visibility, not assumptions about what the security team is handling. If leadership cannot clearly explain what evidence supports their affirmation, that is a control risk, not just a documentation gap.

What the affirmation must be able to support

At the time of affirmation, the organization should be able to produce and defend:

- Evidence of consistent control execution over the preceding year
- Current, updated policies and procedures that reflect the actual operating environment
- Access reviews and system monitoring records
- Incident response testing and documented security activities
- Change management records for any system or environment modifications
- Management oversight and approval documentation

A note for compliance officers:

If you are preparing to sign or support an annual affirmation and cannot readily locate evidence for a significant portion of required controls, that is the most urgent signal that your between-certification program needs structure. The time to act is well before the affirmation is due.

Common Failure Points Between Certification

Across the DIB, certain breakdowns appear consistently in the period following initial certification. Recognizing these early is the difference between manageable drift and a recertification crisis.

Treating compliance as a completed project

After initial certification, organizations de-prioritize compliance activities, reassign compliance-focused staff, and shift attention to other operational demands. When recertification approaches, the team discovers they are effectively starting over.

Consequence:
At recertification, a full remediation effort is compressed into a short window, with elevated costs and contract risk

Inconsistent evidence retention

Evidence collected during the initial assessment is treated as a static record rather than the beginning of an ongoing collection process. Evidence ages, systems evolve, and the documentation no longer reflects actual operating conditions.

Consequence:
Controls that are functionally effective cannot be defended at reassessment because the evidence trail has gaps.

Control ownership drift

Clear ownership of controls exists at the time of initial certification. Over time, personnel responsibilities shift, staff depart, and controls lose their identifiable owners. The institutional knowledge of how controls are executed and where evidence lies walks out the door.

Consequence:
Assessors ask who owns a control, and the answer is unclear, which undermines confidence in the control's ongoing execution.

Untracked environment changes

Systems change, infrastructure updates, and new personnel changes occur without triggering a compliance review. The gap between the assessed environment and the current environment widens silently.

Consequence:
Scope drift and undocumented changes create unassessed risk that surfaces at recertification.

Over-reliance on institutional knowledge

How a control is executed lives in the head of one or two individuals rather than in documented procedures. When those individuals are unavailable, the control cannot be demonstrated or defended.

Consequence:
Single points of failure in compliance operations create audit vulnerability and organizational fragility.

Are You Already Drifting?

Look for these signals:

- Evidence last updated more than 90 days ago
- Controls owners who have left the organization
- System changes not reflected in the SSP
- Leadership preparing to sign an affirmation they cannot fully explain
- Compliance knowledge concentrated in one or two individuals

The Reality of CMMC Moving Forward

CMMC is fundamentally changing how the Defense Industrial Base approaches cybersecurity accountability. The requirement is not going away, and the scrutiny around annual affirmations and recertification evidence is increasing.

Organizations that build continuous compliance discipline into their operations will move through assessments predictably with lower remediation costs, shorter assessment timelines, and stronger contract confidence.

Organizations that continue treating CMMC as a point-in-time event will face the same reckoning every three years: compressed timelines, elevated costs, and the risk of discovering compliance gaps when stakes are the highest.

The three-year window between certifications is not a grace period. It is the compliance program.

Ready to reduce between-certification risk?

Coalfire Federal's CMMC Lifecycle Continuity program is designed for exactly this challenge. Rather than a single assessment every three years, Lifecycle Continuity provides structured validation, repeatable evidence management, and assessment-informed oversight across the full certification lifecycle.

Learn more about CMMC Lifecycle Continuity

COALFIRE FEDERAL

About Coalfire Federal

For 20 years, Coalfire Federal has provided cybersecurity services to a wide range of government and commercial organizations, enabling and protecting their mission-specific cyber objectives. Coalfire Federal is the leading FedRAMP 3PAO and an Authorized CMMC C3PAO, and offers a full spectrum of cybersecurity risk management and compliance services.