PRACTITIONER & EXECUTIVE PAPER • GLOBE-AMERICA CONSULTING, INC.

The G.A.R.D.™ Framework

A Practitioner's Guide to CMMC Assessment Readiness

Eddie White

CMMC Registered Practitioner (RP) • CCP-trained, sitting for certification

Lean Six Sigma Master Black Belt (LSSMBB) • ISO 9001 Lead Auditor

Globe-America Consulting, Inc. • SDVOSB • Fort Worth, Texas

May 2026

Abstract

The Cybersecurity Maturity Model Certification (CMMC) Level 2 assessment process subjects defense contractors to a structured evaluation across three methods, Examine, Interview, and Test, applied to 110 NIST SP 800-171 requirements by independent C3PAO assessors. The dominant vendor response to this challenge has been the development of compliance platforms: software products that automate gap analysis, generate documentation templates, and produce compliance reports. These tools provide real operational value, but on their own they often leave a gap that matters most: the organizational capability to defend implementation claims under direct assessor scrutiny.

This paper introduces the G.A.R.D.™ Framework, Globe-America Consulting's proprietary four-phase methodology. G.A.R.D.™, Govern the Boundary, Align Evidence, Reinforce Implementation, Defend the Assessment, is structured around the same logical sequence that C3PAO assessors follow in the CMMC Assessment Guide. It is designed to complement compliance platforms rather than replace them, by building the organizational readiness that documentation alone cannot produce. This paper describes each phase, explains how methodology and platform investments work together, and presents the framework as a continuous compliance instrument across the full three-year C3PAO certification cycle.

Introduction

There is a gap between compliance documentation and assessment readiness, and it is wider than most defense contractors realize. An organization can have a complete System Security Plan, a documented SPRS score, a library of policies, and a populated POA&M, and still face conditional certification findings that delay contract awards and require significant remediation effort.

The reason is structural. CMMC Level 2 assessments are conducted by independent C3PAO assessors who evaluate not just the existence of documentation, but the verifiable accuracy of every implementation claim against the actual state of the organization's systems. They examine artifacts. They interview personnel. They test configurations. A compliance platform that generates documentation cannot make an IT administrator answer an assessor's question correctly. A methodology can.

G.A.R.D.™ was designed to close that gap. It is a practitioner-developed framework built around the specific demands of the CMMC assessment process, sequenced to address the logical dependencies that determine whether an organization's compliance posture survives contact with an assessor or buckles under it.

Section 1: Platforms and Methodologies, Where Each Earns Its Keep

The defense compliance market has grown significantly in response to CMMC enforcement. The dominant commercial response has been platform development: software products that automate compliance workflows, generate documentation from templates, and provide dashboards for tracking control status across all 110 NIST SP 800-171 requirements. These platforms serve a genuine purpose. They reduce the labor of documentation generation, provide structure for compliance programs, and give organizations visibility across their control landscape. They are valuable tools in a compliance program.

What a platform alone cannot do is make an organization assessment-ready. The distinction matters because CMMC Level 2 assessment is fundamentally an organizational evaluation, not a documentation review. Assessors evaluate three things: whether documentation accurately describes reality (Examine), whether personnel understand and execute the documented controls (Interview), and whether systems behave as documented (Test). Platforms address the first dimension partially, and the second and third dimensions only insofar as the data fed into them is accurate and current.

This is not an argument against platforms. The most successful CMMC programs use both: a platform to manage documentation, evidence inventory, and control tracking, and a methodology to produce the organizational behavior the platform assumes is already in place. The G.A.R.D.™ Framework is the methodology layer. It builds the readiness that platforms can then maintain. Treated this way, the question is not platform or methodology. The question is which methodology turns platform-managed documentation into assessment-survivable posture.

How a platform and a methodology divide the work

Assessment Readiness Dimension	What a Platform Contributes	What G.A.R.D.™ Methodology Contributes
Documentation generation and control tracking	Primary contributor. Templates, workflow automation, and dashboards.	Reviews documentation for accuracy against the actual environment.
Evidence accessibility during assessment	Stores evidence references and links to artifacts.	Verifies every artifact can be retrieved on assessor request.
Personnel knowledge and interview readiness	Limited contribution. Some platforms offer training modules.	Primary contributor. Pre-assessment interviews and walkthroughs.
Configuration accuracy under Test method	Records claimed configurations. Cannot verify they match reality.	Primary contributor. Pre-assessment technical verification testing.

Assessment Readiness Dimension	What a Platform Contributes	What G.A.R.D.™ Methodology Contributes
CUI boundary accuracy	Scopes to inputs provided. Will mirror under-specification.	Primary contributor. Boundary definition and ESP mapping.
Currency across the three-year cycle	Tracks artifact dates and review schedules.	Annual review cycles tied to SPRS affirmation obligations.

Table 1: Division of labor between a compliance platform and the G.A.R.D.™ methodology across the six readiness dimensions that determine assessment outcomes.

The four dimensions a platform alone misses

Organizations that rely on a platform without a methodology layer consistently encounter four assessment vulnerabilities that documentation tools cannot address on their own:

- **Personnel knowledge gaps.** Documentation describes a control. The assessor asks the IT administrator to demonstrate it. The administrator describes a different process than what is documented. The Interview finding contradicts the Examine narrative regardless of how complete the platform-generated SSP appears.
- **Configuration drift.** A platform records that MFA is implemented. The assessor tests it. A service account bypasses MFA enforcement. The Test finding directly contradicts the documented control, raising questions about the accuracy of all other implementation claims.
- **Evidence accessibility.** A platform references artifacts. The assessor requests them. They cannot be produced in current form. Evidence that exists in a platform record but cannot be retrieved during the assessment is treated as non-existent evidence.
- **Boundary accuracy.** A platform scopes the assessment based on inputs provided during setup. If those inputs underspecified the CUI environment, the platform produces documentation that does not accurately reflect the organization's actual compliance scope.

A methodology addresses all four dimensions. It teaches an organization how to govern its boundary accurately, align evidence to every claim, reinforce implementations through verification, and prepare personnel and documentation to defend under assessor scrutiny. G.A.R.D.™ is that methodology.

Section 2: G.A.R.D.™ Framework Overview

The G.A.R.D.™ Framework is a four-phase compliance methodology developed by Globe-America Consulting, Inc. Each phase addresses a distinct dimension of CMMC assessment readiness, and each phase is a logical prerequisite for the next.

Phase Dependency Sequence

01	02	03	04
G	**A**	**R**	**D**
GOVERN the Boundary	**ALIGN** Evidence	**REINFORCE** Implementation	**DEFEND** the Assessment

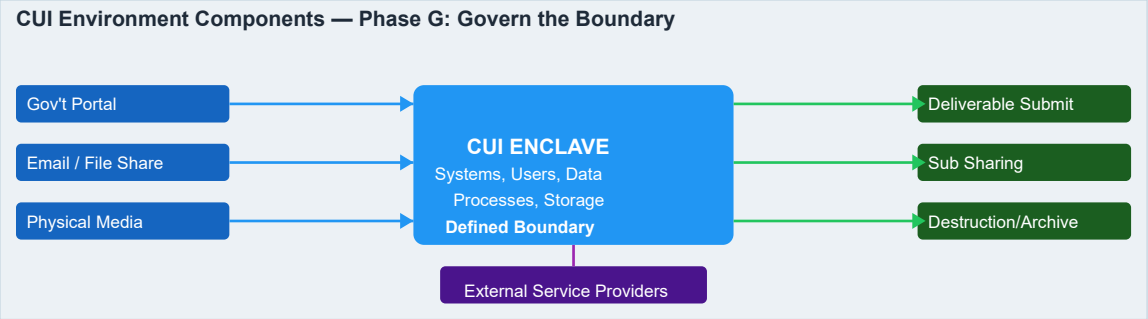
Figure 1: G.A.R.D.™ phase sequence. Each phase produces outputs that are prerequisites for the next.

Framework Design Principles

Principle	Description	Assessment Impact
Sequential Dependency	Each phase depends on outputs from the prior phase. Evidence cannot be aligned before the boundary is governed. Implementation cannot be reinforced before evidence is mapped.	Eliminates wasted effort on documentation that must be revised when boundary or scoping changes occur late in the process.
CAG Method Alignment	Each phase maps directly to one or more of the three C3PAO assessment methods: Examine, Interview, and Test.	Every phase output serves a specific assessment function, ensuring no compliance activity is performed without a direct assessment benefit.
Lifecycle Design	G.A.R.D.™ is structured for continuous application across the three-year C3PAO certification cycle, not as a one-time assessment preparation exercise.	Addresses the annual SPRS affirmation obligation and maintains assessment posture without requiring full re-execution at each cycle.
DIB-Scale Applicability	Designed for organizations with 5 to 200 employees operating without a dedicated compliance team.	Phase outputs are proportionate to the organization's size and CUI environment complexity.

Phase G • Govern the Boundary

The first and most consequential phase of G.A.R.D.™ is Govern the Boundary. Every subsequent phase depends on the accuracy of the work performed here. The boundary governs the scope of the SSP, the applicability of each control, the extent of the evidence required, and ultimately the scope of the C3PAO assessment itself. An inaccurate boundary at Phase G produces compounding errors in Phases A, R, and D.



Defining the CUI Environment

The CUI environment is not synonymous with the organization's IT environment. It is the specific subset of systems, components, personnel, and processes that receive, generate, process, store, or transmit Controlled Unclassified Information. The boundary definition exercise must produce a specific, enumerated inventory, not a generic description, that an assessor can use to independently scope the assessment.

- **Hardware inventory:** All workstations, servers, mobile devices, and network equipment within the CUI scope, identified by name, function, and operating system.
- **Software inventory:** All applications, cloud services, and platforms through which CUI flows, including versions and licensing status.
- **External Service Provider (ESP) relationships:** All third-party services that process, store, or transmit CUI on behalf of the organization, including cloud infrastructure providers (CSPs) and managed service providers (MSPs).
- **CUI data flows:** How CUI enters the environment (government portals, email, physical media), where it is stored and processed, how it flows internally, how it is shared with subcontractors or primes, and how it is disposed of at contract close.

Ownership and Accountability

Phase G must produce a clear accountability structure identifying the owner of every asset within the CUI boundary, the Affirming Official responsible for SPRS attestation, the CMMC Point of Contact (POC), and the designated System Owner. These role assignments are referenced throughout the SSP and are direct targets of assessor interview activities. Personnel who do not know their role in the compliance program, or who describe it differently than it is documented, generate Interview findings.

> **Phase G Key Risk**
>
> The most common boundary error observed across Globe-America Consulting readiness engagements is under-specification of ESP relationships. Organizations routinely document their

on-premises environment accurately and omit the cloud services, email platforms, and collaboration tools through which CUI actually flows. Phase G is complete only when every path CUI travels has been mapped.

Phase A • Align Evidence

With the CUI boundary established, Phase A maps every NIST SP 800-171 control to the specific evidence artifacts that demonstrate its implementation. This phase directly addresses the Examine dimension of C3PAO assessment, and it is the phase where the gap between documentation and assessment readiness most frequently manifests.

The Evidence Map

The evidence map is the operative output of Phase A. It is a structured reference that connects each SSP implementation narrative to specific, accessible artifacts that can be produced during the Examine phase. A well-constructed evidence map enables the following during assessment:

- Rapid evidence retrieval. The assessor requests an artifact, the organization produces it within minutes.
- Gap identification. Any control with no evidence reference is immediately visible as an open item.
- Currency monitoring. Evidence artifacts can be tracked against review dates to prevent staleness.
- SSP narrative validation. Each implementation claim can be cross-referenced against its supporting evidence.

Eliminating Orphaned Controls

An orphaned control is an SSP implementation narrative that makes a specific claim without a corresponding, accessible evidence artifact. Orphaned controls are among the most common sources of assessor findings in CMMC readiness work. They arise in three primary ways:

- **Template inheritance.** SSP language inherited from a vendor template that references generic controls not implemented in the specific organization's environment.
- **Evidence decay.** Artifacts that existed at time of SSP development but have since been deleted, revised, or moved to inaccessible locations.
- **Aspirational documentation.** Implementation narratives written to describe intended future-state implementations rather than the current verified state.

Phase A Completion Criterion

Phase A is complete when every implementation narrative in the SSP has at least one corresponding, accessible evidence artifact that can be produced on request during the assessment. Until this condition is met, the organization has documentation, not assessment-ready documentation.

Phase R • Reinforce Implementation

Phase A produces documentation that accurately describes what should be implemented. Phase R verifies that it is. The critical insight driving Phase R is that documentation accuracy and system accuracy are not the same thing. An SSP can accurately describe the intended implementation of a control. The system can behave differently. When that gap exists, it is discovered during the Test phase of the assessment, not during documentation review.

Pre-Assessment Technical Verification

Phase R consists of a systematic pre-assessment technical verification exercise: testing each claimed configuration against the SSP narrative before the formal assessment. The scope of this verification should cover every control that is subject to the Test assessment method in the CAG, with priority weighting toward the controls most frequently cited in conditional certification findings.

Verification Area	Description	Priority
Multifactor authentication (IA.L2-3.5.3)	Verify MFA enforcement for all accounts, all entry points, and all privilege levels. Specifically test for service account bypass paths, legacy protocol exceptions, and conditional access policy gaps.	**HIGH**
Audit logging (AU.L2-3.3.1 / 3.3.2)	Confirm that audit logs capture all required event types, that retention meets the 90-day minimum, and that logs are protected from modification.	**HIGH**
Access control (AC.L2-3.1.1 through 3.1.22)	Validate least-privilege account configurations, separation of duties for privileged accounts, and remote access controls against SSP claims.	**HIGH**
Configuration management (CM.L2-3.4.1 through 3.4.9)	Verify that system configurations match the baseline documented in the SSP, and that unauthorized software is actively blocked.	**HIGH**

Verification Area	Description	Priority
Vulnerability scan coverage	Confirm that vulnerability scanning covers the full CUI boundary, including all hosts and ESP-managed assets.	**MEDIUM**
Incident response procedure walkthrough	Test the documented incident response procedure with the IR team to confirm execution paths and reporting timelines align with the SSP.	**MEDIUM**
Media protection / removable media policy	Verify enforcement of removable media restrictions and that any approved exceptions are documented and active.	**MEDIUM**
Personnel security awareness	Confirm completion records and content currency of required security awareness training across all in-scope personnel.	**LOWER**

Table 2: Pre-assessment technical verification priorities. Priority tiers reflect the relative frequency with which the corresponding control families produce conditional certification findings in CMMC readiness work.

Ensuring Personnel Execution Matches Documentation

The Interview phase of C3PAO assessment evaluates whether personnel understand and correctly execute the controls documented in the SSP. Phase R addresses this through structured pre-assessment interviews with key personnel: the IT administrator, the CMMC POC, the System Owner, and end users who handle CUI.

The pre-assessment interview serves two purposes. First, it identifies gaps between the SSP narrative and actual operational practice, gaps that must be closed before the formal assessment. Second, it prepares personnel to articulate the organization's compliance posture accurately and confidently in response to assessor questions.

Phase D • Defend the Assessment

Phase D is the integration phase. Its function is to ensure that the work of Phases G, A, and R produces an organization that can survive the C3PAO assessment across all three methods: Examine, Interview, and Test. The operative standard for Phase D completion is straightforward: minimize surprise findings on assessment day.

Mock C3PAO Assessment

The mock assessment is the central activity of Phase D. It is a structured simulation of the C3PAO assessment process, conducted by a qualified CMMC practitioner, that subjects the organization's

compliance posture to the same three-method evaluation it will face in the formal assessment. The mock assessment produces a findings report that identifies contradictions, gaps, and vulnerabilities before they are discovered by the actual C3PAO assessor.

- **Examine simulation.** Document and evidence review against CAG assessment objectives.
- **Interview simulation.** Personnel interviews against documented control implementations.
- **Test simulation.** Technical verification of configurations against SSP claims.
- **Findings report.** Itemized list of contradictions, gaps, and readiness risks.
- **Remediation prioritization.** Ordered list of items requiring closure before formal assessment.

Affirming Official Preparation

The Affirming Official, typically the CEO, President, or COO, bears personal legal accountability for the accuracy of the SPRS score submission under the False Claims Act. Phase D includes a structured Affirming Official briefing that ensures the person signing the attestation understands what they are certifying, has reviewed the pre-affirmation assessment record, and is prepared to accurately describe the organization's compliance program if asked by a contracting officer or investigator.

> **Phase D Affirming Official Standard**
>
> An Affirming Official who signs an SPRS submission without a documented pre-affirmation review has no evidentiary basis for the accuracy of their legal certification. Phase D produces that basis.

Section 3: G.A.R.D.™ Across the Three-Year Certification Lifecycle

CMMC Level 2 certification is valid for three years. Within that period, organizations bear two ongoing compliance obligations: the annual SPRS affirmation, which requires the Affirming Official to certify that the submitted score remains accurate, and the preparation for re-certification at the end of the three-year cycle. G.A.R.D.™ is designed to support both.

Initial Certification	Year 1 Maintenance	Year 2 Maintenance	Year 3 Re-Cert Prep
Full G.A.R.D.™ All four phases	**G → A cycle** Boundary review and evidence refresh	**R phase** Configuration re-verification	**Full D phase** Mock assessment and remediation

Table 3: G.A.R.D.™ activity distribution across the three-year C3PAO certification cycle. The framework is not a one-time checklist; annual affirmation obligations require continuous cycle maintenance.

The Annual SPRS Affirmation

The annual SPRS affirmation is not a passive renewal. It is a legal certification that the organization's compliance posture at the time of affirmation matches the submitted score. An organization whose environment has changed since the prior assessment, through technology migrations, personnel changes, or policy revisions, and which has not maintained its compliance documentation accordingly, is submitting an inaccurate affirmation.

G.A.R.D.™ addresses this through a structured annual review cycle. In Years 1 and 2 of the certification period, organizations cycle through Phases G and A: reviewing the CUI boundary for accuracy, updating the evidence map for any changes in the technology environment or personnel, and confirming that all implementation narratives remain accurate. This review produces the documented pre-affirmation record that supports the Affirming Official's annual certification.

Re-Certification Preparation

In Year 3, organizations execute the full G.A.R.D.™ cycle in preparation for re-certification. The Phase D mock assessment in Year 3 serves a specific purpose: identifying the implementation drift that has accumulated over the certification period and closing those gaps before the formal C3PAO assessment. Organizations that have maintained the Phase G and Phase A cycles through Years 1 and 2 arrive at Year 3 re-certification preparation with significantly less remediation work than those who treat compliance as a point-in-time exercise.

Section 4: G.A.R.D.™ and the NIST SP 800-171 Rev 2 to Rev 3 Transition

This paper is anchored on NIST SP 800-171 Rev 2, the control set on which current CMMC Level 2 assessments are conducted under 32 CFR Part 170. NIST published Rev 3 in May 2024, and the Cyber AB has confirmed that Rev 3 alignment work is in progress with the DoD Program Management Office tracking final guidance from NIST. Defense contractors preparing for assessment in 2026 and 2027 will operate across this transition.

The G.A.R.D.™ Framework is designed to remain stable across the rev change. Its phase logic is structured around the C3PAO assessment process itself, the CAG method dependencies of Examine, Interview, and Test, rather than around any specific list of control identifiers. The boundary work in Phase G applies whether the in-scope environment is being measured against Rev 2 or Rev 3. The evidence alignment in Phase A and the technical verification in Phase R adapt to the active control set without changing the framework's structure.

Where Rev 3 introduces new requirements, particularly the consolidated organizationally-defined parameters (ODPs), the practical impact on G.A.R.D.™ application is contained within Phase A. Evidence maps that previously satisfied Rev 2 implementation narratives will need to be reviewed against Rev 3 ODPs and supplemented where the new control set requires additional evidence. The framework itself

does not change. The artifact inventory expands. Organizations operating G.A.R.D.™ on a continuous lifecycle basis are well-positioned to absorb this transition during their normal Year 1 and Year 2 maintenance cycles, rather than treating it as a separate compliance event.

The recommendation for organizations approaching their first C3PAO assessment in 2026 is to align documentation and evidence to Rev 2 for the assessment of record, while building Phase G and Phase A outputs in a structure that can be extended to Rev 3 ODPs as official Cyber AB guidance issues. This is a content-layer recommendation, not a framework-layer change.

Conclusion

The G.A.R.D.™ Framework is a practitioner-developed response to a specific and persistent failure mode in CMMC compliance practice: the gap between compliance documentation and assessment survivability. Platforms generate documentation. Methodologies build the organizational capability to defend it. The most successful CMMC programs use both.

The four phases of G.A.R.D.™, Govern the Boundary, Align Evidence, Reinforce Implementation, Defend the Assessment, follow the same logical sequence that C3PAO assessors follow in the CMMC Assessment Guide. They address each of the three assessment methods. They are designed for the operational reality of small and mid-size defense contractors. And they are structured for continuous application across the full certification lifecycle, not as a one-time compliance exercise.

Defense contractors who build their compliance programs on G.A.R.D.™ do not simply have documentation that says they are compliant. They have organizations that can demonstrate compliance under direct assessor scrutiny. That distinction is the difference between conditional and unconditional certification, and between a clean assessment and a costly remediation cycle.

About the Author

Eddie White is the founder and Principal Consultant of Globe-America Consulting, Inc., a Service-Disabled Veteran-Owned Small Business (SDVOSB) based in Fort Worth, Texas. He is a CyberAB Registered Practitioner (RP), CCP-trained and currently sitting for Certified CMMC Professional certification, and holds credentials as a Lean Six Sigma Master Black Belt (LSSMBB) and ISO 9001 Lead Auditor. His advisory practice focuses exclusively on CMMC compliance for Defense Industrial Base contractors.

Prior to founding Globe-America, he served 20 years in the United States Air Force, including roles as an Information Security Manager and as a Contracting Officer's Representative (COR) with direct responsibility for government acquisitions and contractor oversight. These assignments provided firsthand experience with the federal regulatory environment, contractor compliance expectations, and the acquisition structures that underpin defense contracting today.

He can be reached at globe-america.com.

References

Cyber AB. (2025). CMMC Assessment Guide Level 2, Version 2.13. Retrieved from cyberab.org.

Cyber AB. (2025, November). November 2025 Town Hall Recap: CMMC Rulemaking Finalized, Enforcement Begins. Retrieved from cyberab.org.

National Institute of Standards and Technology. (2020). NIST SP 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. NIST.

National Institute of Standards and Technology. (2024). NIST SP 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. NIST.

National Institute of Standards and Technology. (2021). NIST SP 800-171A Revision 2: Assessing Security Requirements for Controlled Unclassified Information. NIST.

Department of Defense. (2024). CMMC Program Final Rule, 32 CFR Part 170. Federal Register, Vol. 89, No. 199.

Department of Justice. (2021). Civil Cyber-Fraud Initiative. U.S. Department of Justice.

Defense Federal Acquisition Regulation Supplement. DFARS 252.204-7012; DFARS 252.204-7021: CMMC Requirements.

White, E. (2026). CMMC Phase 1 Is Here: What Small Defense Contractors Need to Know Right Now. Globe-America Consulting, Inc.

White, E. (2026). The SSP as a Living Document: Structure, Evidence Alignment, and Assessment Survivability. Globe-America Consulting, Inc.