CMMC Consulting Services Overview

Independent Readiness Consulting for the Defense Industrial Base

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

About This Overview

This document describes the CMMC consulting services provided by David Koran and Associates. It is written for Defense Industrial Base contractors who are considering a readiness engagement, and for the outside counsel who advise them. The goal is to provide a clear picture of what a consulting engagement looks like, what deliverables come out of it, and what distinguishes this practice from other options in the advisory market.

The practice focuses on readiness. That means the work that precedes a formal CMMC Level 2 certification assessment, not the assessment itself and not the implementation of remediation steps identified during readiness. The reasons for that scope boundary are discussed in the section that follows.

Nothing in this document should be read as legal advice or as a substitute for an engagement. It is an overview. The specifics of any readiness engagement are established during an initial discovery conversation and documented in a written scope of work.

What CMMC Consulting Actually Means

The term CMMC consulting is used loosely across the advisory market. Within this practice it has a specific meaning. Consulting covers the advisory work that precedes a formal certification assessment. It does not include the assessment itself, which only a CyberAB authorized C3PAO can deliver. The distinction matters because the CMMC ecosystem was deliberately structured to separate advisory services from assessment services. A consultant who helps a contractor prepare cannot also certify them. That independence requirement is a feature of the program, not a limitation.

Readiness consulting focuses on three questions. What is the scope of the contractor’s CUI environment. How do existing practices measure against the 110 controls of NIST SP 800-171 Revision 2 that form the basis of CMMC Level 2. What remediation path fits the contractor’s operational reality and timeline. Answering those questions well requires practitioner experience with the specific control families, familiarity with the CMMC Assessment Process document that C3PAOs use, and an understanding of how CMMC interacts with the broader contracting framework including DFARS 252.204-7012, the False Claims Act, and the acquisition rule in 48 CFR.

Scope of Practice

Readiness analysis, gap identification, scope and boundary review, documentation assessment, remediation roadmap development, and SPRS score analysis are all within the scope of this practice.

Out of Scope by Design

C3PAO certification assessments, remediation implementation services, software resale, managed security services, and ongoing operational support are outside the scope of this practice. The boundary is intentional. A readiness advisor who also sells the implementation work that readiness identifies is in a different business than one whose only product is independent analysis. Keeping the practice narrow keeps the analysis independent.

The Readiness Engagement Process

Most readiness engagements follow a consistent sequence. The specifics vary based on contractor's starting posture, complexity of the CUI environment, and target timeline. The structure below describes the typical path.

1. Discovery Conversation

An initial consultation establishes the contractor's current contracts, the CMMC level that applies, the general shape of the CUI environment, and the timeline pressure driving the engagement. This conversation is conducted under confidentiality and results in a written scope of work if the engagement proceeds. The discovery conversation is typically thirty minutes and carries no obligation to proceed.

2. Scope and Boundary Analysis

The most consequential decision in any CMMC engagement is where to draw the assessment boundary. Over-scoping inflates cost and complexity. Under-scoping creates audit failure risk and False Claims Act exposure. This phase maps CUI data flows, identifies the people, systems, and facilities that touch that data, and produces a defensible scope rationale that will survive C3PAO scrutiny. The output of this phase often changes how a contractor thinks about its environment. Many contractors discover that their CUI footprint is either larger or smaller than they initially believed.

3. Gap Analysis Against the 110 Controls

Each control in NIST SP 800-171 Revision 2 is evaluated against current practice. The output is a gap register that identifies which controls are implemented, which are partially implemented, and which are not yet addressed. For each gap, the analysis includes the SPRS scoring implication and a remediation approach proportional to the contractor's operating environment. The gap analysis produces evidence-grade findings, meaning that the implementation status recorded for each control is the status that would be visible to a CMMC Certified Assessor examining the same evidence.

4. Documentation Review

CMMC Level 2 assessment relies heavily on evidence that controls are not only implemented but documented. The System Security Plan, Plan of Action and Milestones, policies, procedures, and supporting artifacts are reviewed against the evidence expectations a CMMC Certified Assessor will apply. Gaps in documentation receive the same treatment as gaps in technical control implementation. The distinction between a control that is not implemented and a control that is implemented but undocumented matters to the contractor differently. Both, however, will show up as findings in a C3PAO assessment.

5. Readiness Report and Remediation Roadmap

The engagement produces a written readiness report that documents the scope decision, the gap register, the SPRS score implication, and a remediation roadmap the contractor can execute internally or with implementation partners. The contractor owns the output. The report is structured for use in conversations with outside counsel, cyber insurance carriers, or prime contractor supply chain compliance teams. The remediation roadmap sequences steps by priority and dependency. Some gaps require foundational work that must precede others. The roadmap makes those dependencies explicit so that the contractor’s leadership can plan the required investment realistically.

Deliverables from a Readiness Engagement

The deliverables from a typical readiness engagement are tangible and usable by the contractor's internal team, outside counsel, and any implementation partners the contractor chooses to engage. The table below summarizes the standard deliverables and their intended purposes.

Deliverable	Purpose
Scope and Boundary Rationale	Documented analysis of CUI flows and resulting assessment boundary, sufficient to defend scoping decisions during a C3PAO assessment.
Gap Register	Control-by-control evaluation across all 110 requirements of NIST SP 800-171 Revision 2, with implementation status, SPRS scoring impact, and remediation approach for each identified gap.
SPRS Score Analysis	Current calculated score, projected score after remediation, and False Claims Act exposure review for any previously submitted scores.
Documentation Assessment	Evaluation of the System Security Plan, Plan of Action and Milestones, and supporting policies against the evidence expectations a CMMC Certified Assessor will apply.
Remediation Roadmap	Sequenced plan of remediation steps, grouped by control family and prioritized against the contractor's timeline and operational constraints.
Readiness Report	Integrated written report suitable for internal leadership, outside counsel, cyber insurance carriers, or prime contractor supply chain compliance teams.

The firm's work stops at readiness. Implementation of remediation steps, ongoing managed services, and the certification assessment itself are all handled by other parties. That boundary is what preserves the independence of the readiness analysis.

Contractor Profiles This Practice Supports

The practice works with DIB contractors across a range of sizes and segments. The common factor is not the industry sector. It is the contractor's position in the CMMC compliance cycle. Readiness consulting is most useful for organizations that have accepted they need to act but have not yet committed to a certification path.

Aerospace and Precision Manufacturers

Contractors producing components to controlled specifications, often holding subcontracts through Tier 1 primes. Scoping is frequently the dominant issue because CUI appears in drawings, specifications, and engineering data that flows through design and production systems. The manufacturing environment creates scoping challenges that do not arise in pure office environments. Machine tools that receive CUI programming files, CAM workstations that interact with CAD systems, and quality inspection equipment that verifies controlled dimensions all present boundary decisions.

Small to Mid-Size Defense Subcontractors

Organizations between twenty and five hundred employees without dedicated compliance staff, where the CMMC obligation lands on a CFO, COO, or IT director who needs analytical support to scope the work and build an internal case for the required investment. This is the most common profile among contractors at the readiness stage. The combination of a CUI obligation and the absence of in-house compliance expertise is what drives most readiness engagements.

Contractors Preparing for SPRS Submission

Organizations that have submitted or are about to submit a self-assessed score to the Supplier Performance Risk System and need independent validation that the score reflects actual implementation. Inaccurate SPRS scores create False Claims Act exposure. A readiness engagement that includes SPRS score analysis produces an independent baseline that a contractor can rely on when affirming the score under the annual attestation requirement.

Contractors Working with Outside Counsel

Engagements where a law firm representing the contractor needs a practitioner advisor to support diligence, remediation planning, or response to prime contractor supply chain inquiries. Work conducted at the direction of counsel benefits from appropriate privilege considerations. Engagements with outside counsel are structured so that the practitioner work product supports the legal analysis the firm is conducting rather than operating as an independent deliverable.

How Engagements Are Structured

Every engagement begins with a discovery conversation. That conversation is free of charge and carries no obligation. Its purpose is to determine whether a readiness engagement is appropriate for the contractor's situation and, if so, to establish the scope of work.

A scope of work document is produced following the discovery conversation. The scope of work specifies the phases of the engagement, the deliverables, the timeline, and the fees. Fees are established on either a fixed-fee or hourly basis depending on the predictability of the scope. Contractors with a well-defined CUI environment typically receive fixed-fee proposals. Contractors with less defined environments typically begin on an hourly basis for the initial scoping phase and move to fixed-fee proposals for subsequent phases once the scope is understood.

All engagements are conducted under confidentiality. When the engagement involves handling Controlled Unclassified Information during the course of the work, appropriate handling arrangements are established before any CUI is shared. The practice maintains a FedRAMP-authorized Google Workspace enclave for CUI handling when required.

Deliverables are the property of the contractor. The contractor retains the right to share readiness work product with counsel, insurance carriers, primes, or any other party at its discretion. The practice does not retain work product beyond what is necessary for its own professional records and does not reference contractor-specific engagement details in any public content without explicit permission.

Questions Contractors Ask Before a First Call

Is this the same as a C3PAO assessment?

No. A C3PAO assessment is the formal third-party certification assessment conducted by a CyberAB authorized organization. Readiness consulting is the advisory work that prepares a contractor to undergo that assessment successfully. The two activities are performed by different parties. A practitioner cannot both advise a contractor and certify them, and an assessor cannot provide readiness consulting to a contractor they will later assess. That separation is built into the program.

Do we need CMMC Level 1 or Level 2?

Level applies based on the data involved in a contract. Level 1 applies to contracts involving Federal Contract Information only. Level 2 applies to contracts involving Controlled Unclassified Information. The determination is contract-specific and often not obvious. The discovery conversation addresses this question directly. Getting the level determination correct is usually the first readiness decision.

How long does readiness work typically take?

Readiness engagements vary based on the contractor’s size and complexity. A small contractor with a contained CUI environment and reasonably current documentation may complete readiness analysis in a matter of weeks. A mid-size contractor with distributed CUI flows, legacy documentation, and multiple business systems involved may require several months. Estimating the timeline accurately is part of the discovery conversation.

Can we share the readiness report with a prime contractor?

Yes. Readiness reports are the contractor’s work product and are structured to be shareable with prime contractor supply chain compliance teams, outside counsel, or cyber insurance carriers. Contractors increasingly face supplier compliance inquiries from their primes, and an independent readiness report provides a credible response to those inquiries.

What about implementation? Do you fix the gaps?

Implementation is a separate activity performed by the contractor's internal team, an IT managed service provider, or a specialized implementation partner. The readiness engagement produces the remediation roadmap. The contractor chooses who executes it. This separation preserves the independence of the readiness analysis and avoids the conflict that would exist if the party identifying gaps were also the party selling the remediation work.

What happens if our SPRS score is wrong?

Inaccurate SPRS scores create False Claims Act exposure. The readiness engagement includes review of any previously submitted SPRS score against actual implementation and identifies any material discrepancies. Correction of an inaccurate score is a matter for the contractor's counsel to advise on. The readiness analysis provides the factual foundation for that conversation.

Do you work with our law firm?

The practice regularly supports outside counsel advising DIB contractors on cybersecurity obligations. Engagements conducted at the direction of counsel can be structured with appropriate privilege considerations. Work for law firms is one of the practice's standard service patterns.

About the Practitioner

David W. Koran is the founder of David Koran and Associates, a consulting practice focused on CMMC readiness for Defense Industrial Base contractors and the legal counsel who advise them.

David holds the CyberAB Registered Practitioner Advanced credential and is an Associate Member of the American Bar Association Section of Public Contract Law. He is the author of *The CMMC Decision*, now in its second edition, a practitioner reference covering the decisions contractors face when evaluating their CMMC path.

The practice focuses on readiness, enablement, and implementation guidance for DIB contractors. It does not conduct C3PAO assessments, sell software, or resell managed services. That independence is central to how the practice operates.

Contact

dkoran@davidkoran.com

(802) 335-2662

davidkoran.com