WIZ | RISCPoint

From Readiness To Resilience: A Guide To CMMC Success And Cloud-Ready Defense

Cut through the complexity of CMMC with practical guidance, technical strategies, and clear steps to navigate the accreditation ecosystem

Table of Contents

Executive Summary

Navigating the Cybersecurity Maturity Model Certification (CMMC) ecosystem requires a deeper understanding than just the standard itself. For organizations that interact with data in-scope, including but not limited to a small subcontractor handling basic federal data, a prime contractor managing high-value assets, a research institution, and everything in-between.

The reality is that successful achievement of certification will be required to demonstrate cybersecurity maturity to avoid losing access to broad markets, including federal contracts, grants, subcontracts and in certain cases with large prime contractors, all opportunities.

With evolving rules, interrelated frameworks like FedRAMP, and a maze of technical and legal requirements, many organizations are asking: Where do we start — and how do we get it right the first time?

This white paper cuts through the noise and breaks down the essentials—what CMMC level you need, how to determine if you're handling Controlled Unclassified Information (CUI), how to scope your environment, and how to build a future-proof compliance strategy.

Along the way, we explore powerful accelerators — like CNAPP platforms and enclave-based architectures that can speed up your journey without sacrificing sustainability. You'll also learn how to engage the right partners, avoid common pitfalls, and design a program that does more than pass a certification audit — it provides real-world security and defense in-depth.

If your business interacts with federal data, this paper is your roadmap to clarity, compliance, and competitive advantage.

I. What CMMC do you need?

The Cybersecurity Maturity Model Certification (CMMC) is a long-discussed program overseen by the Department of Defense (DoD) and intended to increase the United States' cybersecurity posture within its Defense Industrial Base (DIB).

The program establishes three maturity levels, each was designed to provide minimum cybersecurity controls commensurate with the risk of the data that is being handled by the contractor and its sub-contractors*.

The DoD defines risk within the CMMC final rule 32 CFR Part 170 as the measure of the extent to which an entity is threatened by a potential circumstance or event. It goes on to define risk as typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs, and (ii) the likelihood of occurrence.

Below is an illustration of each level:

CMMC Level	1- Foundational	2- Advanced	3- Expert
Scope:	Contractors who only handle Federal Contract Information (FCI)	Contractors & subcontractors who handle Controlled Unclassified Information (CUI)	Contractors & subcontractors supporting high-value assets or performing work critical to national security
Requirements:	17 basic safeguarding practices	110 Technical Controls & Practices from NIST SP 800-171	Level 2 C3PAO certification & additional NIST SP 800-172 controls against Advanced Persistent Threats (APTs)
Assessment Approach:	Self- Attestation	Self-Attestation** or C3PAO Certification	Level 2 C3PAO Certfication & additional DIBCAC Audit

Note, as of this publication, Level 3 remains in a preliminary state. While the Department of Defense has outlined its intent for Level 3 to support the most sensitive workloads, the final control set, assessment procedures, and timeline for implementation are still under development. No organizations have been formally assessed against Level 3 to date. However, defense contractors working on Special Access Programs (SAP) or with critical technology IP should begin evaluating their readiness for eventual Level 3 requirements.

*CMMC is a mandatory contractual flow-down unless the prime contractor or subcontractors can evidence that they will not store, process, or transmit scoped data.
**Only Available when handling CUI not otherwise specified

II. What is CUI?

To navigate the CMMC ecosystem effectively, it is crucial to develop a strong understanding of CUI, its purpose and the intricacies associated with the broad data classification. Whether your contract requires self-attestation or a C3PAO assessment, the presence — and proper handling — of Controlled Unclassified Information is the primary driver of your CMMC obligations.

The Technical Definition

Controlled Unclassified Information (CUI) is defined by the National Archives and Records Administration (NARA) as:

"Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies, but is not classified under Executive Order 13526 or the Atomic Energy Act."

CUI encompasses a broad range of sensitive information types, including but not limited to:

- Export-controlled data
- Engineering specifications
- Legal documents
- Procurement and acquisition data
- Sensitive personally identifiable information (PII)

The *CUI Registry*, maintained by NARA, organizes CUI into categories and subcategories. Working with your prime contractor or United States Contract officer, contractors work to understand the types of CUI and specific Law, Regulation or Government wide policy that governs the CUI they will be interacting with.

CUI in Layman's Terms

In simple terms, *CUI is information the government wants to control, but does not feel rises to the risk of requiring classification*. Think of it as sensitive-but-shareable, CUI can include drawings for parts on a military vehicle, internal schedules for a federal agency, or budget spreadsheets that, if exposed, could create risk.

III. How to know if you have CUI?

The Technical Lens

Determining whether your organization handles CUI requires a technical and contractual analysis. CUI is not always labeled or obvious — it may be embedded in technical drawings, shared via collaboration tools, or delivered as part of contract deliverables. CUI originates from the federal government or is created by contractors on behalf of the government under specific contracts.

To determine if you have CUI, review:

- **Your contracts and DFARS clauses** — specifically DFARS 252.204-7012, which mandates protection of CUI.
- **Statements of Work (SOWs) and Performance Work Statements (PWS)** for references to sensitive deliverables.
- **Markings and metadata in documents** — look for labels such as "CUI"
- **Subcontractor flow-downs** — CUI responsibilities may be passed down from a prime contractor.

A Practical Approach

- **Start with your contracts:** Identify any relationships or contracts where you directly or indirectly work with the United States Government and therefore, may receive or create CUI
- **Enhance your data inventory (or create it):** Once you've identified potential sources of CUI, work to integrate it into your data Inventory, or if your organization does not maintain a data inventory, utilize CMMC to start the journey to identify all types of data your systems store, process, or transmits and start with the data classification of CUI.
- **Collaborate with your customer:** If you've determined that you may hold CUI, seek clarity with your Government Contract Officer, or with your Prime customer's Information Security department to seek clarity and alignment as to what CUI is.
- **Leverage Technology and a trusted advisor:** DSPM Compliance and cybersecurity consultants can help conduct a data flow and classification analysis.

Failing to recognize the presence of CUI is one of the most common causes of CMMC non-compliance. Taking a proactive, structured approach to identifying CUI in your environment is not only the best practice —it's a critical foundation for selecting the right CMMC level and building an effective compliance strategy.

IV. Scope of Boundary

CMMC is unique in the world of compliance as the boundary of certification is prescribed (e.g., FedRAMP) but also allows for strategic design (e.g., SOC 2 and ISO). Ultimately, the Certification is required for where you'll store, process and transmit CUI, and you can choose to extend this to your organization, limit it to a properly segmented enclave or build and go-to market with a bespoke CMMC External Service (see do you need FedRAMP in the coming sections). Improperly scoped assessments of CUI environments have historically been an area of risk within the space and when designing your CMMC environment presents a key decision point.

How do you decide what is right for you? Determining whether to certify your entire organization or create a purpose-built enclave. This decision is both strategic and operational. It depends on your organizational structure, the scope of your federal contracts, the complexity of your systems, and your long-term business goals. Each approach carries trade-offs in cost, effort, and flexibility.

Full Organizational Certification

- Best suited for companies where federal work is core to operations.
- Provides the most flexibility in handling CUI across teams and systems.
- Requires a unified implementation of all required controls organization-wide.

Enclave-Based Certification

- Ideal for companies with limited or segmented federal exposure.
- Reduces the scope of systems, users, and processes subject to CMMC requirements.
- Enables faster, more focused implementation with lower cost and complexity.

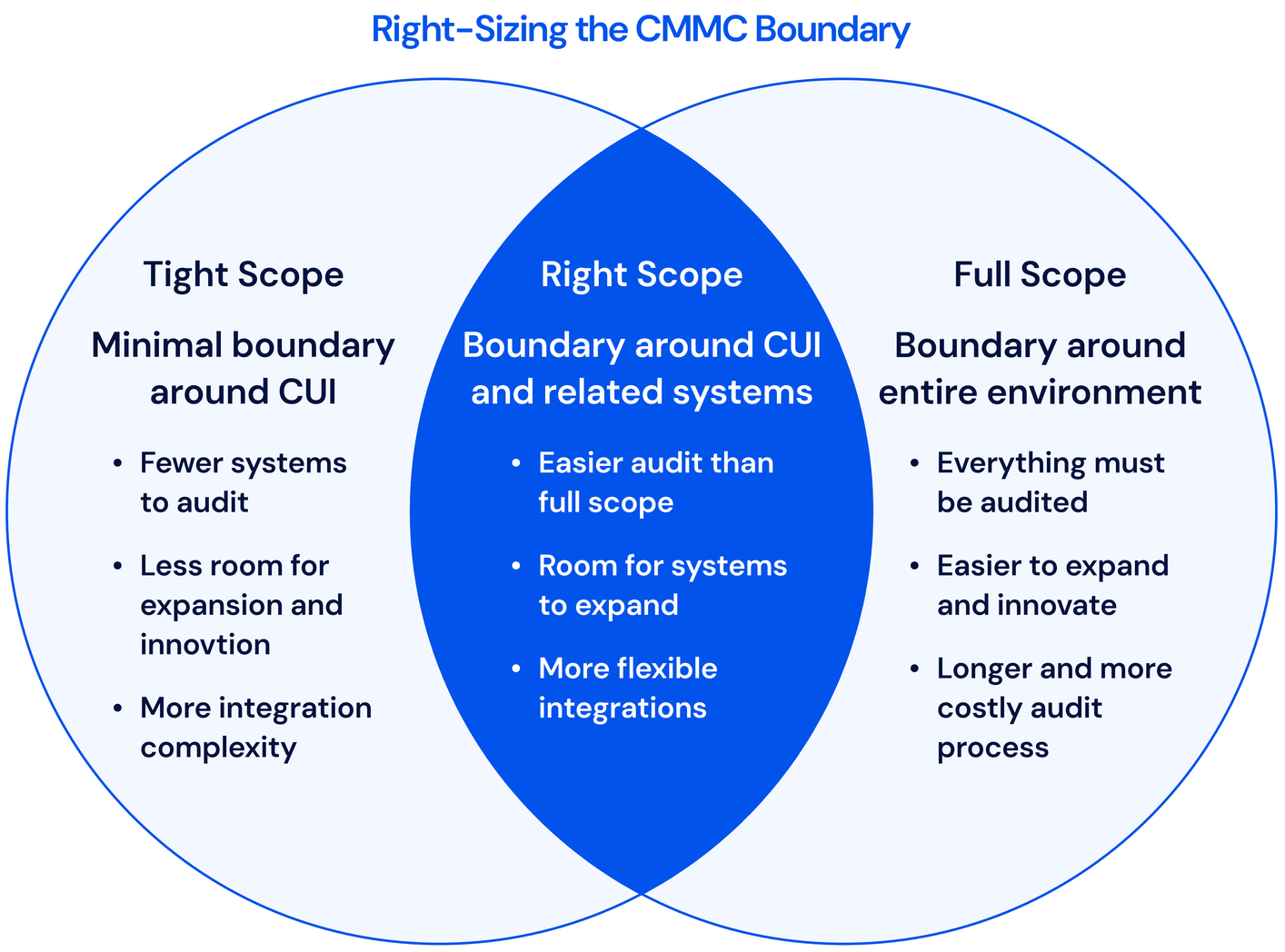
To help facilitate an analysis organizations should:

- Assess the systems, processes and people involved with CUI to determine if an enclave is technically feasible
- Evaluate whether isolating CUI-related activities is feasible while meeting contractual business needs.
- Engage compliance and technical experts to design a right-sized boundary.

An enclave approach often provides an efficient path to compliance—particularly when paired with cloud-native tooling and zero trust architectures—but it must be carefully planned to ensure long-term success.

Why the Boundary Matters

A tightly scoped boundary reduces assessment burden but may introduce integration complexity. Over-scoping drives cost and increases overarching risk as a larger attack surface is harder to manage and an increased audit footprint creates a more complex compliance journey. Right-sizing the boundary is an art—requiring partnership between engineering, compliance, and legal teams.



Understanding the Data Flow

Ultimately, your evaluation should produce a clear path to CMMC compliance and at a minimum the starting point of critical artifacts, including system boundary diagrams, user authentication flows, and of course, data flow diagrams that help show the systems directly storing CUI and those indirect systems that are critical to your CMMC environment.

These systems may not be obvious without such an exercise and level of documentation. Holistically this package should help provide clarity of your boundary, technology architecture, and control implementation and avoid scoping and audit failure.

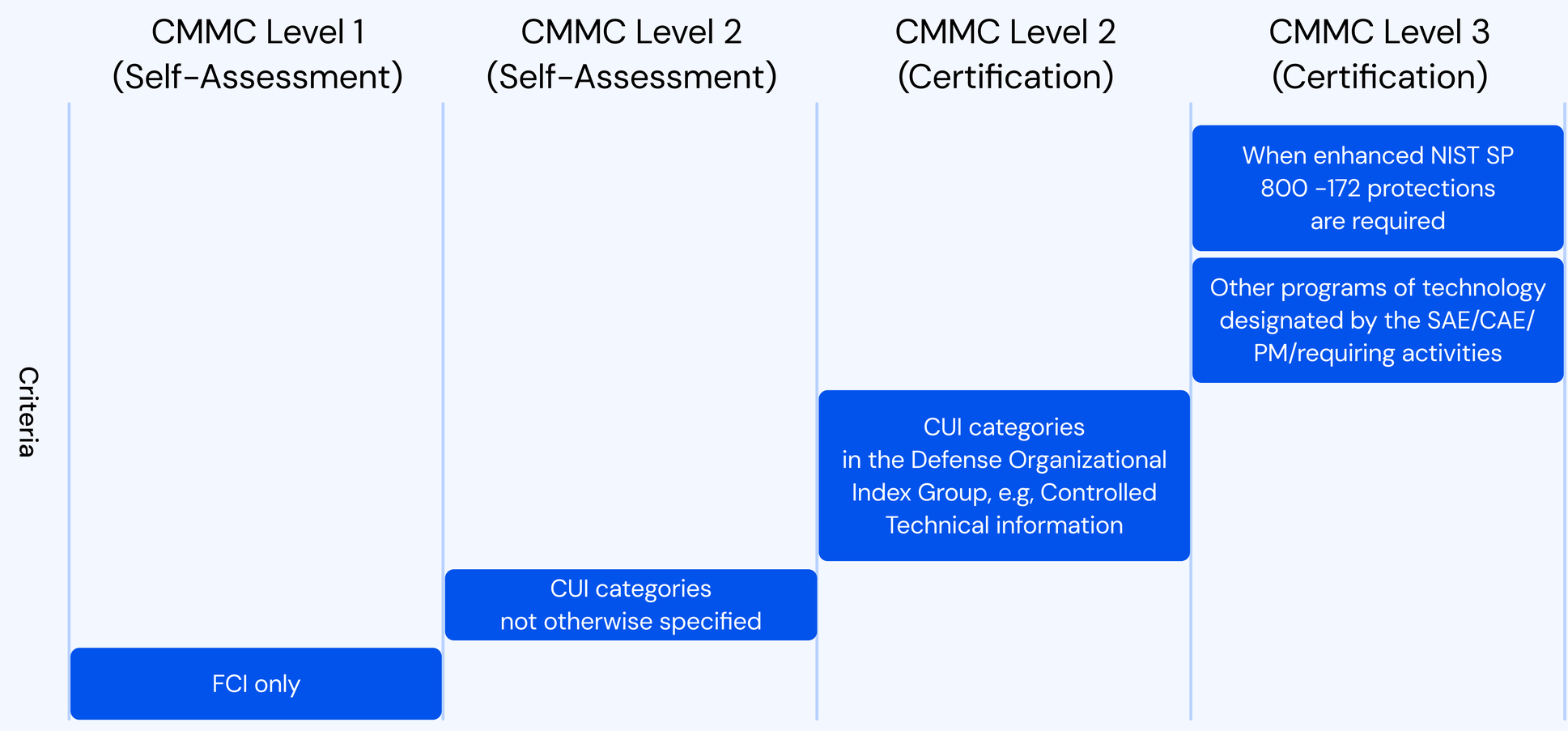
V. Determining CMMC Level

The CMMC Level you'll have to meet is relatively simple to determine given the clear guidance from the department of defense. If you'll only store, process or transmit FCI, Level 1 and self-assessment is all that is required***.

When your contract includes the handling of CUI things become a bit more complex. Not only does level 2 introduce additional control requirements, it brings with it complexity as to whether you can self-assess or require external C3PAO certification. Generally speaking, the majority of Level 2 contractors will require a C3PAO certification. The Department of Defense recently released a Level Determination guide and specified that only CUI categories not otherwise specified would qualify for self-assessment.

For Level 3, you'll be working closely with your Mission Owner or Contract Owner and know that you'll be subject to a Level 3 assessment, however, if you are an organization that is evaluating contracts with the potential to require Level 3 assessments, you should start with a Level 2 certification as that will be a prerequisite regardless

CMMC Level Determination Guide



CUI: Controlled Unclassified Information
CAE: Component Acquisition Executive
FCI: Federal Contract Information
PM: Program Manager
SAE: Service Acquisition Executive

***While Self-Assessment for level 1 is all that is required it is still recommended that you engage with an advisor or assessor to minimize risk of a false claim.

Do you need FedRAMP?

FedRAMP and CMMC are both United States Government programs intended to protect data. FedRAMP's scope is the protection of Federal Data within Cloud Service Offerings, whereas CMMC's (level 2 for the purposes of this discussion) scope is CUI in a non-federal system.

Where confusion often occurs is the requirement for a CMMC Level 2 certified environment to only leverage External Cloud Service Providers (CSPs) that are FedRAMP Moderate, FedRAMP Moderate Equivalent, or greater (FedRAMP High), this intermingling of frameworks can lead to confusion, and it's important to understand each framework separately, then how they interrelate.

FedRAMP Authorization:

- Purpose: To efficiently authorize Cloud Service Offerings (CSOs) for use by United States Executive Agencies.
- Scope: The Cloud Service Offerings (Authorization Boundary)
- Key Considerations: Authorization requires an executive agency customer (Agency Partner), all interconnected services must also be authorized

CMMC Level 2 Certification:

- Purpose: To certify a non-federal system has adequate cybersecurity controls to provide appropriate protection for CUI
- Scope: The environment where the contractor will store, process and transmits CUI, including external service providers
- Key Considerations: Utilizing External CSPs requires the use of a FedRAMP Moderate Authorized or Equivalent services.

FedRAMP Moderate Equivalence:

- Purpose: Bespoke process allowing Cloud Services to provide services to CMMC certified environments that are not FedRAMP Authorized
- Scope: The Cloud Service Offering (Authorization Boundary)
- Key Considerations: Requires "Perfect" assessment, meaning at the time of the Equivalence no control deviations or vulnerabilities can exist within the system. Does not require an Executive Agency Partner.

When should you seek FedRAMP Moderate Equivalence? Simple, if you do not sell to United States executive agencies and do not have a clear path to a United States Executive Agency Partner, but your customers will require CMMC you'll need to maintain FedRAMP Moderate Equivalence. The benefits of seeking equivalence over a FedRAMP Moderate Authorization to Operate (ATO) is usually a shorter timeline and cost, however it is worth noting achieving FedRAMP Moderate Equivalence still requires nearly all of the same effort as receiving a FedRAMP Moderate ATO. Many organizations may start with Equivalence, and then submit for FedRAMP authorization to expand their potential target audience.

VI. How to Navigate the CMMC/Accreditation Ecosystem

Cutting through the Noise- You can't just buy CMMC

Given the complexity of CMMC, it is tempting to "Buy" CMMC compliance, and there is a large number of organizations that promise just that, and while there are manners to accelerate your journey, no magic bullet exists. Be a ware of those advertising this approach.

That is why we recommend finding the right trusted advisor for your journey. They will help you find the right tools, processes and plans to prepare for your ultimate assessment, the initial advisor should act as your coordinator and quarterback, key questions to ask include:

- How do you help your clients evaluate organizational vs. enclave certification
- What toolsets are you familiar with and certified in
- Do you utilize templates or create a bespoke approach
- Do you have a network of assessors you've worked with, who are they are how do you determine which are the right fits for your customers

Technology Accelerator- Automating Visibility and Risk Assessment

Demonstrating CMMC compliance requires accounting for where CUI data resides, and complete visibility for all connected resources to identify indicators of risk. This visibility with context can require intensive manual work unless technologies are leverages which can automate data and risk assessment. For cloud environments this automation can be accomplished through a Cloud-Native Application Protection Platform (CNAPP).

A modern CNAPP can replace multiple legacy point solutions such as cloud security posture management (CSPM), container/Kubernetes security posture management (KSPM), cloud infrastructure entitlement management (CIEM), cloud workload protection (CWP), vulnerability scanners, code scanners, malware scanners, and others.

CNAPPs use cloud-native APIs to continuously scan public cloud environments and inventory deployed resources. These can include networking components, VMs, containers, data repositories, identities, AI, and others. At the same time, a mature CNAPP will identify indicators of risk such as vulnerabilities, misconfigurations, malware, exposed secrets, and deviations from key frameworks like Defense Information Systems Agency (DISA) Security Technical implementation Guides (STIGs) and Center for Internet Security (CIS) Benchmarks. By analyzing these data in a graph database, CNAPPs uncover toxic combinations and prioritize remediation guidance based on the likelihood of compromise.

This approach helps organizations align with CMMC requirements by providing continuous monitoring, contextual risk evaluation, and actionable insights to reduce exposure across cloud environments. These insights can help organizations to focus on the most critical issues first, to quickly identify and remediate the greatest exposure risk. For example, a CNAPP would discover and prioritize an exposed secret tied to an overly permissive role on a public-facing workload with access to a data repository housing CUI over a separate workload with several Common Vulnerabilities and Exposures (CVEs) but which does not lead to a sensitive data bucket.

Modern CNAPPs are extending this automated discovery and risk prioritization to traditional on premises environments, including vSphere deployments.

Automating Compliance Reports

In addition to helping organizations to proactively identify and remediate areas of greatest risk within their cloud environments, CNAPPs can help alleviate some of the compliance reporting requirements posed by CMMC assessments.

These include:

- Custom data classification rules to quickly identify CUI data patterns within the environment, and all connected cloud resources to help identify the appropriate scope boundary
- Automated discovery and reporting of all CVEs within the environment
- Automated reporting of adherence to technical baselines including DISA STIGs and CIS Benchmarks
- Automated generation of inventoried technologies and a software bill of materials (SBOM)
- Democratization of Security
    - CNAPPs can extend security across an organization to democratize security by enabling teams that traditionally fall outside of the security organization to have a positive impact on security while also accelerating their mission effectiveness. CNAPPs accomplish this democratization in several ways:
    - Shifting security left into the CI/CD pipeline and into the developer Integrated Development Environment (IDE) to bring the same policy scanning into code and accelerating time to production readiness
    - Shifting security right into the Security Operations Center (SOC) through automated threat detection and runtime event augmentation with cloud context to more efficiently and accurately identify indicators of compromise with the necessary forensics for root cause analysis and potential blast radius

Process Accelerator

The rush to get CMMC Certification can lead to processes that are built solely to check boxes — technically satisfying controls but failing to create a secure, scalable, or sustainable operating environment. This often leads to compliance debt: a condition where poorly designed or hastily implemented processes result in higher maintenance costs, audit risks, and operational inefficiencies down the road.

The key to avoiding this trap is to work with experienced compliance architects who understand how to balance urgency with intentionality. Rapid certification should not come at the expense of alignment with your actual business workflows, team structures, and technical ecosystem.

Rather than duplicating existing processes or force-fitting controls, a strategic process accelerator approach:

- Prioritizes automation and repeatability
- Aligns policies with actual practices — not theoretical models
- Emphasizes continuous improvement, not one-time compliance

Organizations should recognize that not every control can be solved by technology. Many require carefully crafted human processes, such as:

- Role-based access reviews
- Incident response workflows
- Secure development lifecycle checkpoints
- Third-party vendor due diligence

By investing in tailored, risk-aligned process design, companies can achieve compliance faster — without creating a parallel universe of artificial policies that teams ignore after the audit is over.

Not every control is solved by technology. While there are key controls that you can meet with technologies, there is no true silver bullet or easy button that will satisfy every control for you. Making the right selection and building a sustainable program and environment is critical in the sustained speed to market.

Partnership with your C3PAO

It is critical to engage your Certified Third-Party Assessor Organization (C3PAO) early — well before the formal assessment begins. The most reputable C3PAOs act as true partners in the process, not just evaluators at the finish line. Early collaboration enables mutual understanding of scope, expectations, and readiness indicators.

Working with a C3PAO from the start allows your organization to:

- Establish a realistic timeline with shared milestones
- Clarify interpretation of specific CMMC requirements
- Preemptively identify potential areas of noncompliance or control gaps
- Avoid last-minute surprises and costly rework

Experienced assessors will often support a phased engagement model, offering pre-assessment reviews or readiness consultations to build alignment and reduce ambiguity. This not only creates a smoother certification experience but also improves the quality and defensibility of your audit outcomes.

Independent C3PAOs — like Schellman — bring added value through transparency, consistency, and credibility —ensuring your compliance program is built not just to pass inspection, but to stand up to scrutiny over time.

VII. In it for the Long Haul

Leveraging partnerships to Maintain Innovation and Accreditation

Compliance is not a static goal—it is a continuous journey. The same partnerships that accelerate your path to certification must also be leveraged to sustain your authorization over time. Ongoing collaboration with technology providers, process advisors, and C3PAOs ensures that your compliance program evolves in parallel with your infrastructure and business objectives.

Long-term success requires more than annual check-ins. It involves integrating partners into your change management cycles, reassessing control effectiveness regularly, and anticipating regulatory updates that may impact your authorization scope.

Continuous Monitoring (CONMON)

Achieving compliance is just the beginning. Continuous Monitoring — or CONMON — is a cornerstone of both FedRAMP and emerging CMMC expectations. CONMON refers to the real-time or near-real-time tracking of security controls, vulnerabilities, configuration changes, and threat detection.

As your environment evolves, so too must your compliance posture. Key scenarios that may require reassessment or reauthorization include:

- Introduction of new technologies (e.g., containers, AI/ML integrations)
- Expansion of CUI boundaries or data flow changes
- Organizational changes impacting governance or ownership
- Infrastructure or hosting changes (e.g., moving between cloud regions)

A mature CONMON strategy ensures you remain audit-ready, avoid lapses in authorization, and demonstrate continuous risk management to your customers and federal stakeholders.

Security doesn't end at the compliance assessment. As infrastructure changes or new features roll out, continuous monitoring (CONMON) ensures alignment with authorization requirements. Reassessment may be necessary as your boundary evolves.

A sustainable security and compliance posture can also be accelerated and maintained by using some of the following best practices:

- Secure Software Supply Chain/secure by design
    - Preemptively identify and eliminate high-severity risks within the CI/CD pipeline prior to production deployment
    - Integrating compliance into DevOps without deployment of agents or requiring manual processes

Enhanced visibility from code to cloud connects code repositories to production environments for unified security and posture management, by unifying code and cloud security posture management, code production readiness can be accelerated. This acceleration is achieved by reducing or eliminating reliance on siloed scanning tools and providing developers the necessary context to identify and fix issues before code is committed.

Compliance Resiliency through Best Practices Foundations

Achieving certification is a milestone—but sustaining compliance is a discipline. Compliance resiliency refers to an organization's ability to withstand operational, regulatory, and technological changes without jeopardizing its security posture or accreditation status. Some of the items below define the importance of compliance resilience and how it's critical in maintaining your CMMC and overall compliance program.

Key Components of Compliance Resiliency:

1. Technology Enabled Boundary: CMMC's authorization Boundary is unlike any other in the public sector space. Utilizing a technology which allows for real-time monitoring and provides automation to keep you up to date will ensure sustainable compliance and prevent surprises at the assessment that can lead to substantial emergency remediation effort. Utilizing technology to support your boundary also provides the strongest evidence for purposes of your C3PAO validation.

2. Policy-to-Practice Alignment: Effective compliance programs are built on real-world policies that reflect how the organization actually operates—not aspirational documents created solely for audits. Ensure policies are actionable, accessible, and embedded in day-to-day processes.

3. 3. Cross-Functional Ownership: Security is no longer confined to the IT department. Compliance resiliency requires shared accountability across security, engineering, HR, procurement, and executive leadership. Establishing a governance council or compliance steering committee can help reinforce enterprise-wide alignment.

4. Threat-Informed Practices: As threats evolve, so must your controls. Organizations should map their control framework to threat models (e.g., MITRE ATT&CK) and leverage cyber threat intelligence to inform proactive risk mitigation — especially where CUI or mission-critical functions are involved.

5. Continuous Skills Development: Human error remains a leading cause of breaches. Invest in role-specific training for system administrators, developers, executives, and users. Tailored security education ensures stakeholders understand their responsibilities and stay vigilant.

6. Documentation Discipline: Maintain robust documentation that evolves with your environment—including asset inventories, data flow diagrams, access logs, incident response playbooks, and evidence of control operation. Consistent documentation practices simplify audits and support defensibility under scrutiny.

7. Integrated Change Management: Ensure that compliance is factored into every change — whether it's a new vendor, a cloud migration, or a code deployment. Integrate compliance checkpoints into DevOps and business transformation processes to avoid retrofitting security after-the-fact.

8. Resilient Supply Chain Assurance: Vet your vendors and require contractual flow-downs for CMMC-relevant obligations. Establish a third-party risk management (TPRM) program that includes periodic reassessments, especially for IT service providers and software vendors involved in CUI workflows.

By grounding your compliance strategy in operational best practices and aligning it to your risk posture, organizations can move beyond short-term certification goals toward a resilient and defensible cybersecurity posture that supports long-term growth and public sector trust.