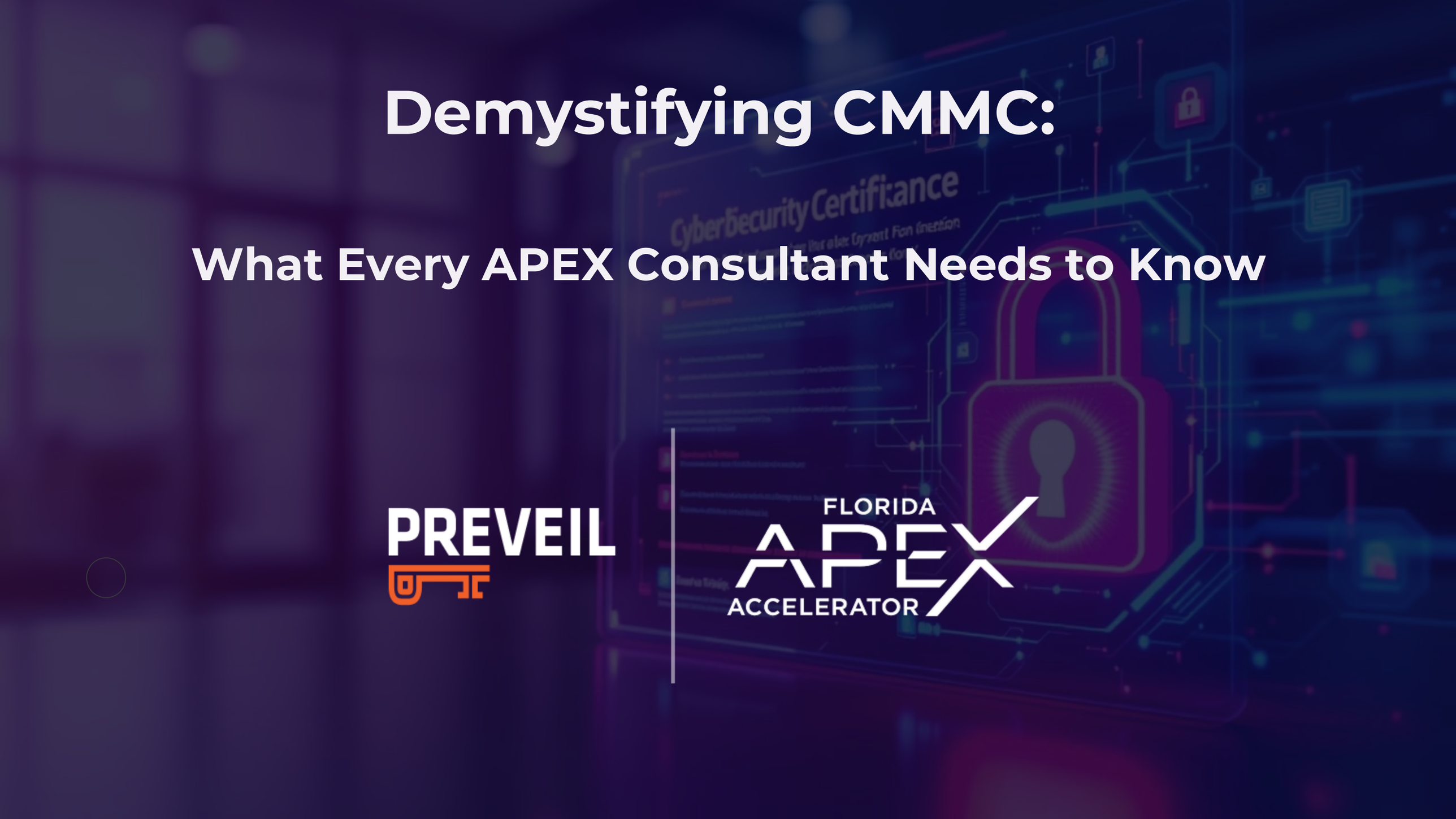
Demystifying CMMC:

What Every APEX Consultant Needs to Know



PREVEIL

FLORIDA APEX ACCELERATOR

Agenda

What is CMMC and who it applies to

Understanding the fundamentals of the Cybersecurity Maturity Model Certification and identifying organizations that need to comply.

Key compliance requirements

Exploring the essential controls, documentation, and processes needed to achieve CMMC certification.

Real-world case study

Examining successful implementation strategies through an actual defense contractor example.

PreVeil's compliance platform

Introduction to specialized tools designed to simplify CMMC compliance for defense contractors.

Q&A

Addressing specific questions related to CMMC implementation and compliance strategies.

This session will provide APEX consultants with practical knowledge and resources to support defense contractors through their CMMC compliance journey, from initial assessment to certification.

What is CMMC?

- The Cybersecurity Maturity Model Certification (CMMC) is a comprehensive framework established by the Department of Defense in 2019
- Its primary purpose is to safeguard Controlled Unclassified Information (CUI) that resides on defense contractors' networks and systems.
- It is is a validation of compliance with the DFARS 7012 requirements regarding NIST 800-171 implementation.
- Contractors who process, store, or transmit CUI will be expected to self assess, annually, and have a CMMC 3rd Party Assessor Organization (C3PAO) complete a full assessment, every 3 years.

The Role of DFARS 252.204-7012

NIST 800-171 Implementation

Requires defense contractors to implement 110 security controls outlined in NIST SP 800-171 to adequately protect CUI.

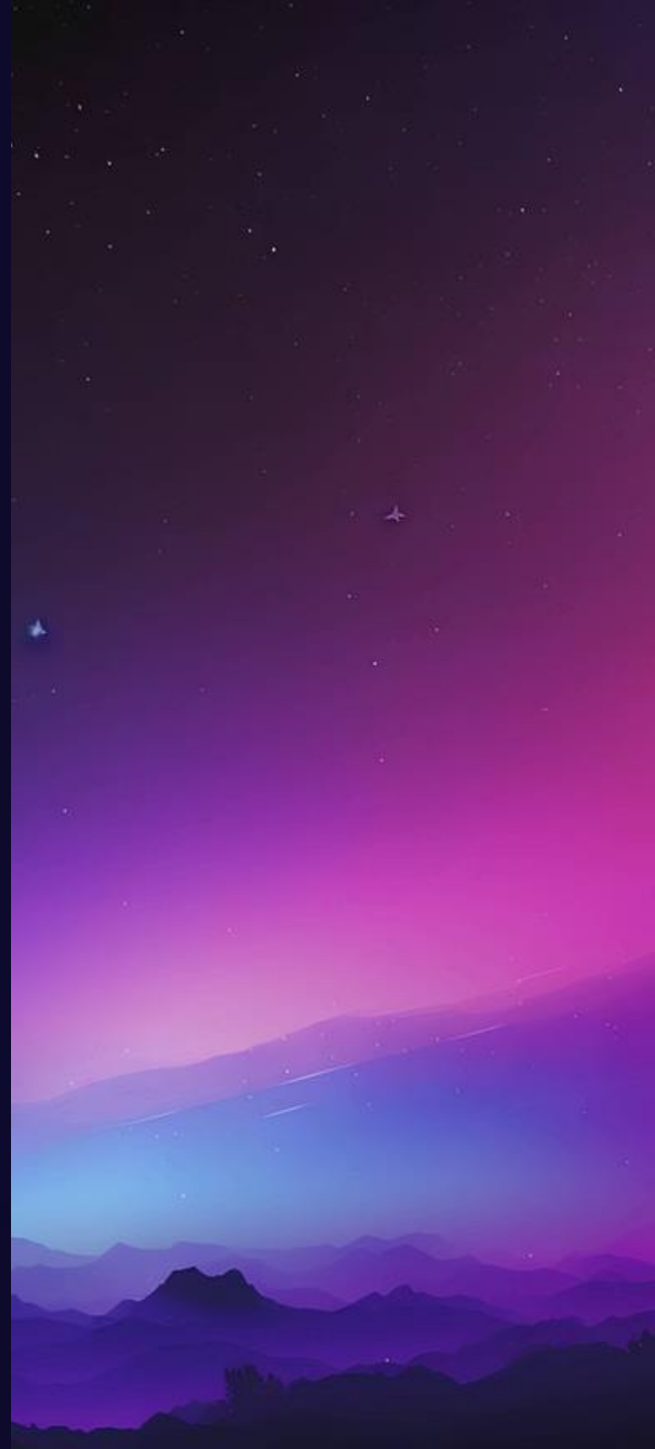
72-Hour Incident Reporting

Mandates that contractors report cyber incidents affecting covered systems within 72 hours of discovery.

FedRAMP Moderate Cloud Solutions

When using cloud services, contractors must ensure they are equivalent to FedRAMP Moderate baseline security controls.

DFARS 252.204-7012 has been the regulatory foundation for DoD cybersecurity requirements since 2017, but CMMC brings increased accountability through mandatory verification of compliance.



Who Needs to Comply with CMMC?

Defense Contractors Handling Sensitive Information

Any organization that processes, stores, or transmits Controlled Unclassified Information (CUI) as part of DoD contracts.

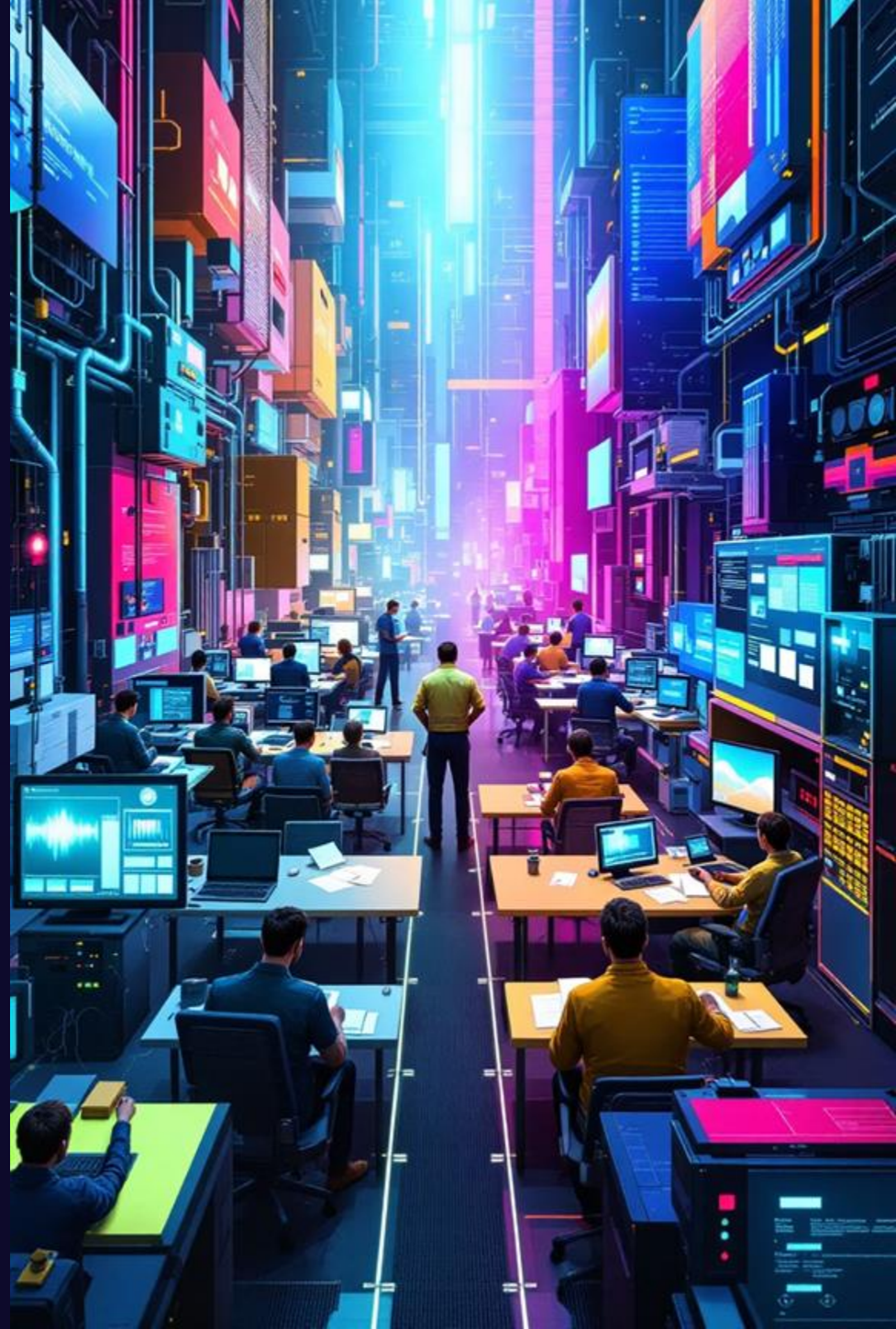
Prime Contractors, Subcontractors, and MSPs

The requirements flow down through the entire supply chain, affecting prime contractors, subcontractors, and the Managed Service Providers (MSPs) that support them.

Over 220,000 Companies in the DIB

The Defense Industrial Base encompasses a vast network of organizations, from large defense primes to small specialized manufacturers and service providers.

Critical consequence: Non-compliance with CMMC will result in ineligibility for DoD contract awards, potentially eliminating significant revenue opportunities for affected businesses.



CMMC Is Here: Timeline and Implementation

December 2024

CFR 32 Final Rule established the CMMC program officially, solidifying the regulatory framework and requirements.

1

2

January 2025

CMMC assessments began, with early adopters seeking certification to maintain competitive advantage in DoD contracting.

3

Coming Soon

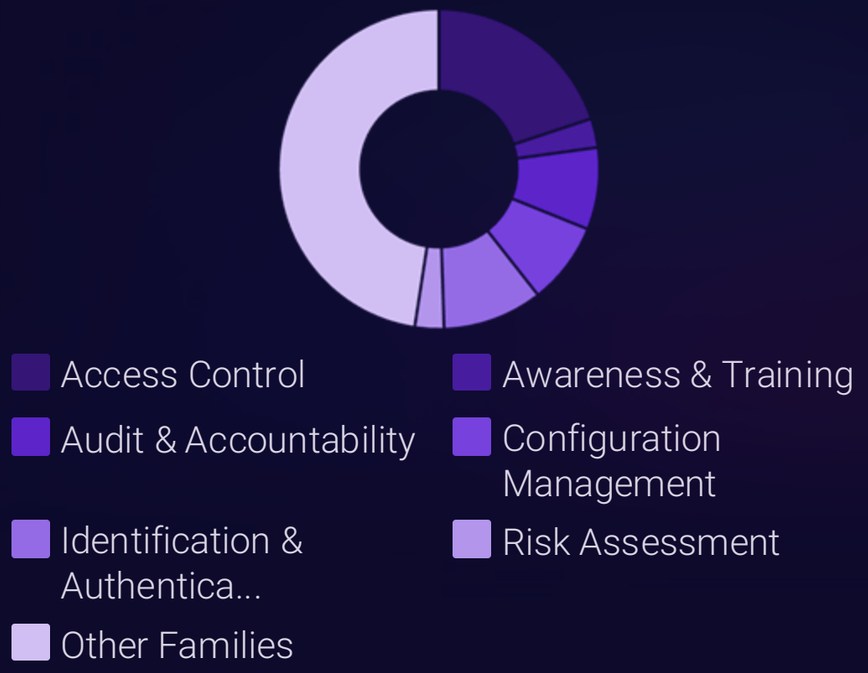
CFR 48 rule expected to insert CMMC requirements directly into contracts, making compliance mandatory for award eligibility.

Many contractors incorrectly believe CMMC implementation is years away. The reality is that the program is active now, and organizations that delay preparation risk losing eligibility for future contracts. The time to act is immediately, as assessment slots with authorized C3PAOs are already filling up.

> Waiting until CMMC appears in contract requirements will be too late - organizations need 6-12 months on average to prepare for assessment.

What's Required to Meet CMMC Level 2

Compliance requires a holistic approach integrating technology, people, and processes. It's not merely implementing software tools but establishing a comprehensive security program.



Core Requirements

110 NIST controls distributed across 14 security families

Over 320 assessment objectives that must be satisfied

Technical safeguards: Encryption, access control, multi-factor authentication

Documentation: System Security Plans (SSPs), Plans of Action & Milestones (POA&Ms), policies and procedures

Training programs: Regular security awareness training for all personnel

Helpful Resources

The following resources can significantly streamline the compliance process and increase the likelihood of successful assessment:

GRC Platforms

Governance, Risk, and Compliance platforms help track control implementation status, manage evidence collection, and monitor ongoing compliance posture.

CMMC Consultants

Experienced consultants and Registered Practitioners can provide guidance, conduct gap assessments, and develop remediation strategies tailored to your organization.

Templates and Accelerators

Pre-built policy templates, assessment worksheets, and compliance accelerators can reduce documentation time and ensure alignment with CMMC requirements.

Readiness Assessments

Preliminary evaluations identify gaps in your security posture before official assessment, allowing for targeted remediation and increased confidence.

Key Players in CMMC Ecosystem

Cyber AB

The official CMMC Accreditation Body responsible for training and accreditation from C3PAOs and individual assessors. They establish assessment methodologies and maintain the CMMC ecosystem.

APEX Accelerators

Formerly PTACs, these organizations provide technical assistance to small businesses navigating federal contracting requirements, including CMMC compliance.

C3PAOs

CMMC Third-Party Assessment Organizations conduct official assessments to verify compliance with CMMC requirements and issue certifications to qualifying contractors who receive a 110/110 on their CMMC Level 2 assessments..

DIBCAC

The Defense Industrial Base Cybersecurity Assessment Center is the DoD's internal assessment team that conducts assessments and provides oversight of the CMMC program.

Project Spectrum

A DoD initiative providing free training resources, tools, and guidance to help small and medium-sized contractors understand and implement cybersecurity requirements.

As APEX consultants, you play a crucial role in connecting smaller contractors with appropriate resources and guidance. Many small businesses lack the internal expertise to navigate CMMC requirements effectively.

CMMC in the Real World: Case Study

Envision Success Story

Envision, a small manufacturing contractor successfully achieved CMMC readiness through strategic partnerships and a methodical approach:

- Partnered with a specialized CMMC consultant to develop an implementation roadmap
- Saved 90% over the cost of GCCH
- Deployed PreVeil's secure email and file-sharing platform to protect CUI
- Achieved compliance with all 110 security control objectives
- Successfully passed a CMMC assessment, validating their security posture

> *"We knew we had to get our data into a FedRAMP compliant cloud and it basically came down to PreVeil and GCC High. We got the GCC High quote and it was just crazy: It was over $200,000 for 33 users...the PreVeil quote was 1/10th of that. We were really impressed in the demo—it checked so many of the boxes, so that's the route we went"*

Jonathan Carr
Director of Technology & CISO

Envision
Innovative Solutions

Envision's journey demonstrates that with proper planning, appropriate technology solutions, and expert guidance, defense contractors of any size can successfully implement CMMC requirements.

Check out the full case study: **https://www.preveil.com/envision-case-study/**

Introducing PreVeil

PreVeil is an **encrypted email and file sharing platform** used by **over 1700 defense contractors** to protect their CUI and meet CMMC requirements without overhauling their existing infrastructure. To date, PreVeil has **enabled 25+ defense contractors, MSPs and C3PAOs** to achieve a 110/110 on their CMMC assessments.

Encrypted File Sharing + Email

Protects CUI without oververhauling existing systems. Seamlessly integrates with Office 365, GSuite, Outlook, Gmail and Exchange

CMMC Compliance Accelerator

Detailed, pre-filled, customizable documentation with videos and tutorials to simplify achieving compliance.

Network of Trusted Partners

Access our network of C3PAO and consultant experts to refine your documentation and streamline your assessment

PreVeil’s Network to Support APEX Teams

Co-Marketing Opportunities

Access to 25+ free events per year, 20k attendees, 100% free.

Dedicated Sales, Compliance + Partner Team

Our internal teams offer a variety of services to help accelerate your customer’s compliance journey. From free 15-minute compliance calls to in depth platform training – where here to help.

Get started today!

Get started by downloading a free copy of PreVeil. Just go to our website (preveil.com) and click on the Get Started menu

FINIS

FLORIDA APEX ACCELERATOR

- Luis Batista
- lubatist@fiu.edu
- Phone: 305-814-2584

PREVEIL

- Noël Vestal
- complianceinfo@preveil.com
- Phone: 857-957-0345