

CMMC V2 Certification Guide

**A Simple Guide to Comply with the DoD's Cybersecurity Maturity Model Certification
(CMMC)**

Background

Keeping Controlled Unclassified Information (CUI) secure from prying eyes is critical to our national sovereignty and economy. Yet companies that process important government data (whether directly or as a sub-contractor in the supply chain) have only been required to “self-attest” to their conformance with relevant DFARS/NIST SP 800-171 guidance.

Unfortunately, that didn't work very well ...



A low-angle shot of a large, classical-style building with many columns and windows, reaching towards the sky. An American flag is flying in the foreground on the right side, partially obscuring the building. The flag is waving in the wind.

The Problem

“The U.S. is losing \$600 billion a year to our adversaries in exfiltrations, data rights, & R&D loss. If we were able to institute good cyber hygiene and reduce that by 10%, think of the amount of money that we could save to truly reinvest back into our partners in the industrial base that we need to stay on the competitive edge...”

KATIE ARRINGTON , FORMER SPECIAL ASSISTANT FOR CYBERSECURITY TO ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION

The Solution

CMMC will require each organization to “prove” they are fully compliant by a combination of;

- 1) Entering a score in SPRS
 - 2) A Senior Official signing an attestation of conformance
 - 3) Undergoing a C3PAO certification assessment
-

CMMC V2 Level 2: 110 Security Requirements Across 14 Security Domains

Access Control

Awareness & Training

Audit & Accountability

Configuration Management

Identification & Authentication

Incident Response

Maintenance

Media Protection

Personnel Security

Physical Protection

Risk Assessment

Security Assessment

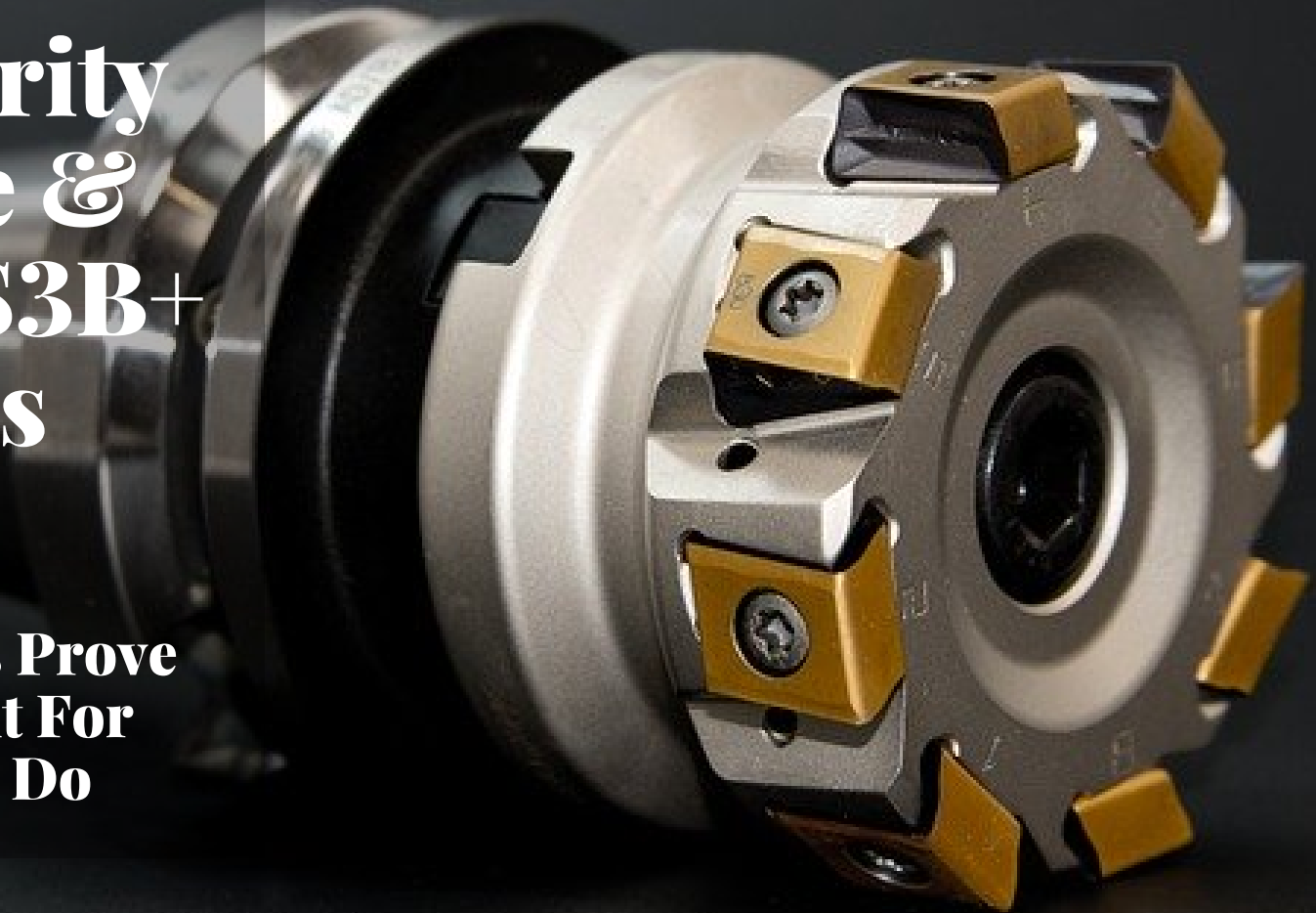
System/Communications Protection

System & Information Integrity

**That's Where
We Fit In...**

**Pivot Point Security
Has “Been There &
Done That” for \$3B+
of Manufacturers
& Suppliers...**

**We Have Been Helping Firms Prove
They Are Secure & Compliant For
Over 20 Years... It's What We Do**



This isn't our first rodeo.

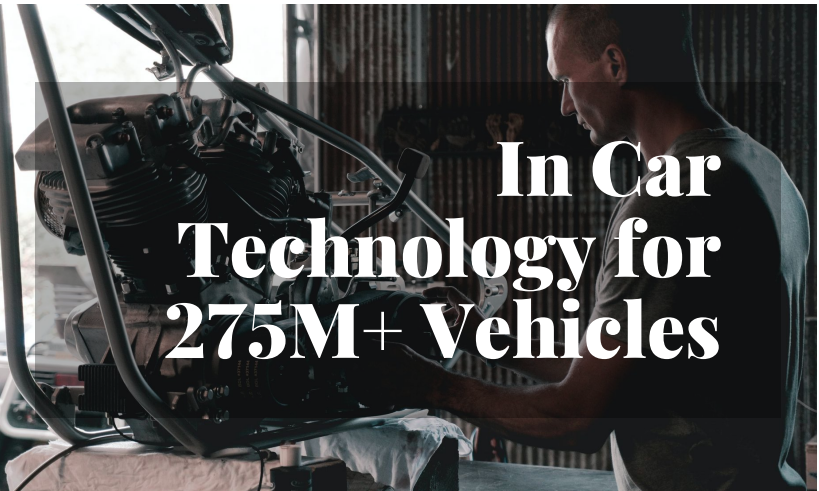
Our confidence comes from our experience and all that we are trusted to protect...

A photograph of a SpaceX Falcon Heavy rocket launching, with a large plume of smoke and fire. In the background, a large white building with the SpaceX logo and an American flag is visible.

CMMC/800-171 for \$3B+ Manufacturers

A close-up photograph of a barcode with the number 374 255000 printed below it.

**The World's
Barcodes**

A photograph of a man working on a car engine in a workshop.

**In Car
Technology for
275M+ Vehicles**

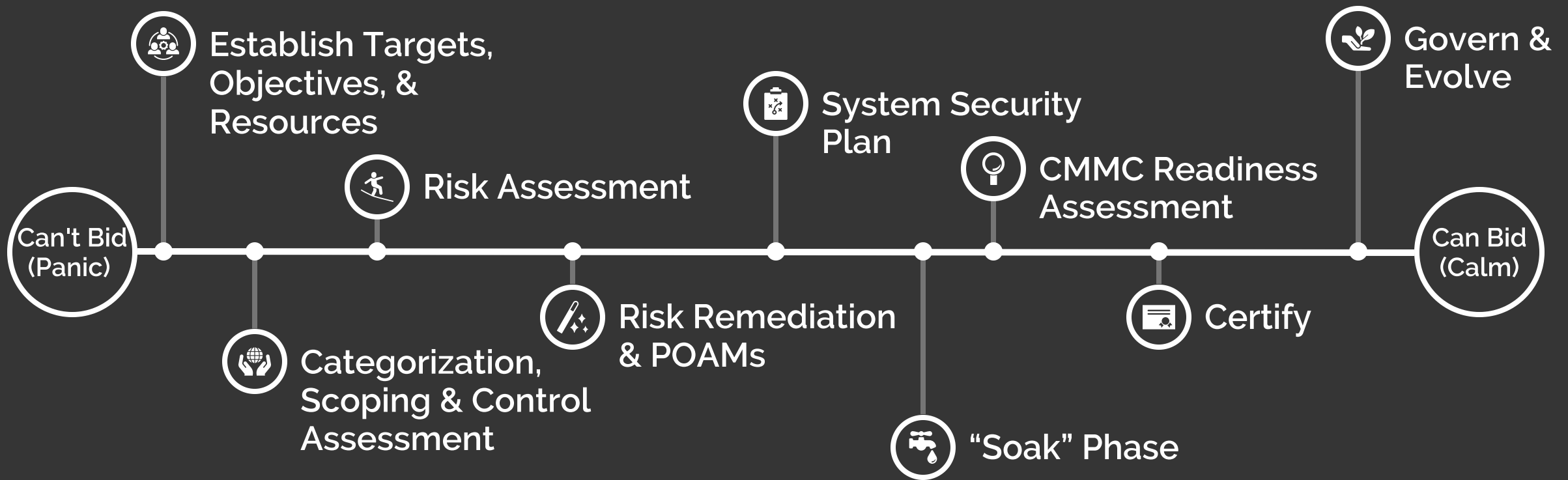
A photograph of three people sitting around a table, looking at documents and a laptop.

**100+ ISO 27001
Certifications**

An aerial photograph of a large, modern government building complex.

**200+
Government
Entities**

Lean on Our Proven Process to Achieve CMMC Certification





Step #1: Establish Targets, Objectives, & Resources

Establish CMMC Level, Time-Frame, & Resourcing

Ask yourself these questions:

What CMMC Level do I need?

You may need to consult with an upstream agency or prime contractor for guidance. If you are uncertain, CMMC Level 2 achieves full 800-171 conformance and is likely your target.

When do I need to get certified by?

<6 months (if you are not 800-171 compliant already) will be a challenge.

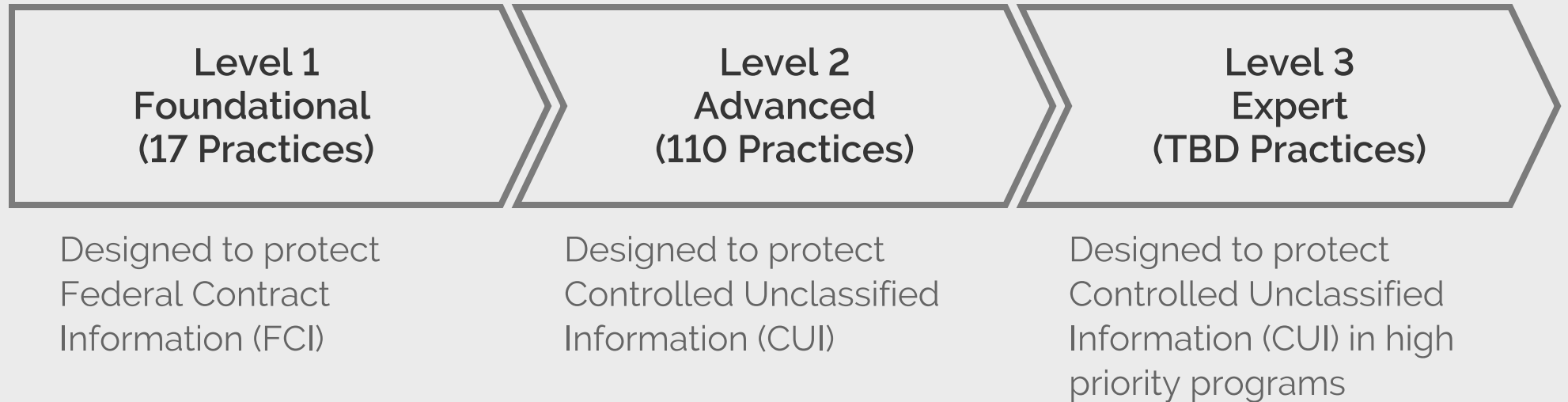
What personnel, expertise, & financial resources do I need to get certified?

Most importantly, do you have the internal expertise and bandwidth to achieve DFARS 7012/7019/7020 or 7021 compliance in your target time frame?



CMMC “Cyber Hygiene” Certification Levels

Gain a Better Understanding of What the CMMC Level You Need Entails





Step #2: Scoping & Control Maturity Assessment

Understand Where Controlled Unclassified Information (CUI) Controls are Required & How to Segregate/Protect Each Asset Type

Review relevant artifacts (e.g., existing policies, network diagrams) and conduct scoping interviews to understand how your CUI flows to, within, and from your organization. At the same time assess the maturity of CMMC relevant controls. Use this information to categorize and classify your assets and establish the scope of your CMMC SSP.



Step #3: Risk Assessment

		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
Likelihood ↑	Very Likely	Low Med	Medium	Med Hi	High	High
	Likely	Low	Low Med	Medium	Med Hi	High
	Possible	Low	Low Med	Medium	Med Hi	Med Hi
	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
	Very Unlikely	Low	Low	Low Med	Medium	Medium

Know (& Prove to the CMMC Assessor) That All Key Risks to CUI are Understood and Effectively Managed

Establishing a repeatable methodology for, and conducting a Risk Assessment no less than annually, is a CMMC requirement. Leverage the results of the Scoping/Control Maturity Assessment to identify control implementation gaps that are leaving you at an “unacceptable” level of risk and/or non-compliant with CMMC.



Step #4: Risk Remediation & POAMs

Build & Execute the Risk Treatment Plan That Will Lead to Successful CMMC Certification

Leverage the Risk Assessment to determine and identify/document the control implementation gaps that need to be addressed for you to move you to your target state into an actionable Risk Treatment Plan.

Roles of Users and Number of Each Type:

Number of Users	Number of Administrator Privileged Users
0	3

Description of Information: Engineering, Inc. processes, stores, and Technical Information, DoD Critical Infrastructure Security Information, Propulsion Information, and Unclassified Controlled Nuclear Information.

ENVIRONMENT

Engineering, Inc. designs and manufactures motion control components for the Defense and manufacturing take place in both our Boca Raton, FL and Needham Heights, MA facilities. Engineering, Inc. also hosts servers that process and store CUI in AWS Govcloud.



Step #5: System Security Plan (SSP)

Document “How” Your CMMC Compliant Systems Protects CUI

CMMC requires that you develop an SSP that “provides an overview of the security requirements of the system, describes the controls in place for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system.”



Step #6: “Soak” Phase

SPRS & Time to Build The Evidence for Your C3PAO Assessment or Self Attestation

With your SSP documented, your controls in place, and POAM's for those controls that still are in progress, you are ready to get a score in SPRS to meet your DFARS 252.204.7019/7020 requirement. As you work through POAM's you will update your score in SPRS to reflect your current status

A CMMC assessor will be looking for at least two forms of objective evidence that each of the 110 practices is operated in a “persistent and habitual” manner.



Step #7: CMMC Readiness Assessment

Document “How” Your CMMC Compliant Systems Protects CUI

Ensuring you have what you need for a successful CMMC certification assessment or your self attestation is best done by validating your readiness via a readiness assessment. Just make sure the person (inside your organization or outside) is objective enough to audit the environment and is either an accredited Registered Practitioner (RP), Certified CMMC Professional (CCP), or CMMC Certified Assessor (CCA).

Control Objective	Reasonably-Expected CMI
<p>ations for all physical access points (nts) to the facility where the system resides</p> <p>ility officially designated as publicly</p> <p>zations before granting access to the</p> <p>ining the system using physical access</p> <p>designated as publicly accessible in</p> <p>assessment of risk;</p> <p>ther physical access devices; and</p> <p>hen keys are lost, combinations are nsferred or terminated.</p>	Individual access authorizations are ver facility.
	Access is controlled to areas based on t requirements.
	Keys, combinations, and other physical
	When lost, or when individuals are tran changed when that individual likely had
	When compromised, or when individual combinations are changed when that in combination.
	Visitors are issued a physical token (e.g. <ul style="list-style-type: none"> - Identifies the visitors as not onsite per - Must be surrendered before leaving the and - Expires through automated or visual m day).
<p>agement, operational, and technical e work sites;</p> <p>ness of security controls at alternate work</p> <p>o communicate with information security nts or problems.</p>	As part of the Business Continuity Plan (work sites.
	Plan addresses maintaining adequate s work sites.
	Plan addresses the effectiveness of secu
	Plan addresses the approved means for security personnel in case of security in



Step #8: Attest or Get Certified

Submit Your Attestation or Engage a C3PAO

Once the cybersecurity program has been implemented, and appropriately documented, it is CMMC Assessment and self attestation ready.



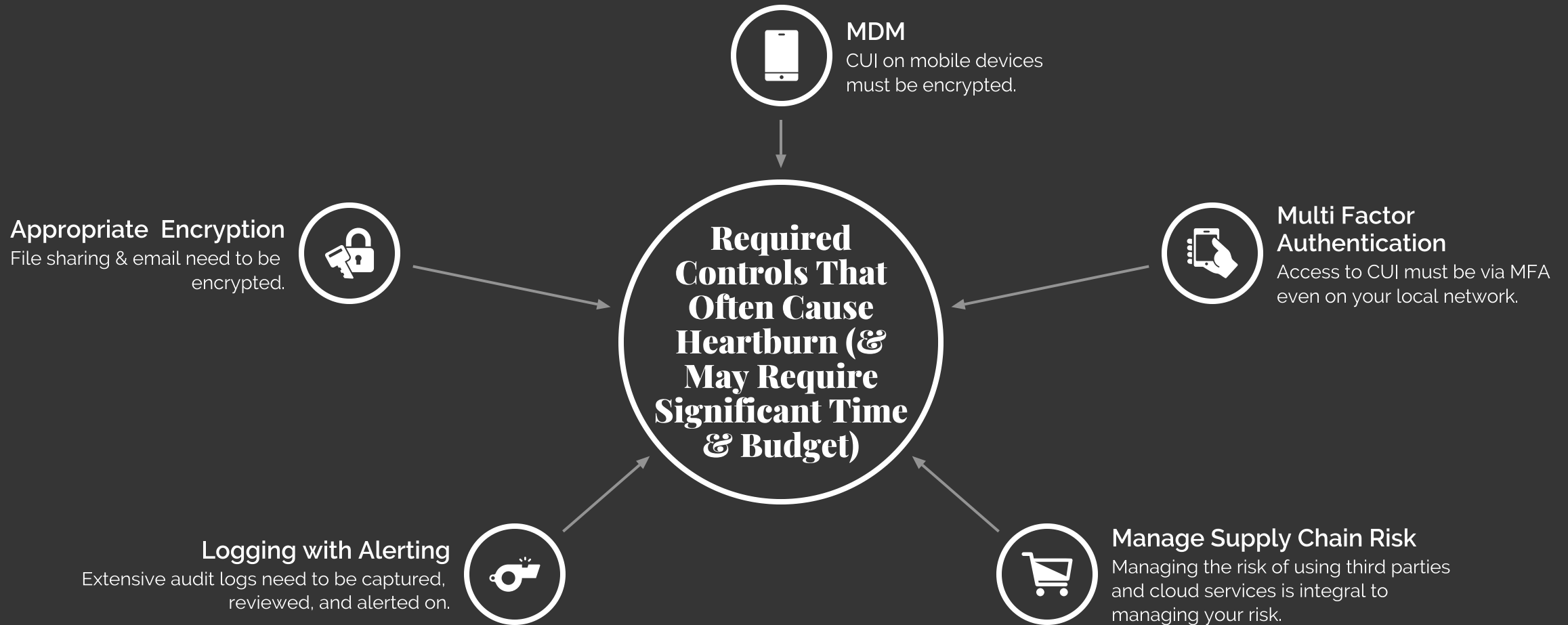
Step #9: Govern & Evolve

Maintain Your Attestation/Certification via Continuous Monitoring & Continuous Improvement

Once you attest and/or are certified you will be required to provide ongoing (yet to be formally documented) evidence that you are maintaining compliance with CMMC.



Beware of these CMMC “Gotcha’s”





What Would Non-Compliance With CMMC Look Like For You?

What would happen to your customer count and sales numbers if you could no longer win new DoD contracts?



What Would Non-Compliance With CMMC Look Like For You?

What about the Whistleblower act and the False Claims Act?

Are disgruntled employees a compliance risk to your organization?

Would a DIBCAC audit have civil liability implications?

If You Follow Our Proven Process, Successful CMMC Should Feel Like This...



Get excited!

**You can continue to bid on
and win DoD projects.**

Get Even More Excited!

**Not all firms that
currently compete with
you for DoD contracts
will be successfull in
their CMMC pursuit,
leaving you with
more room to grow.**

Get even more & more excited!

**Reading the writing on the
wall, other government
agencies are considering the
CMMC as their de facto
standard to bid on federal
contracts. You will be primed
to find additional federal
contract work outside of the
DoD.**

Life is Risky... Working with us to achieve CMMC Compliance/Certification isn't!

CMMC Information Straight from the Source

EP#1 KATIE ARRINGTON – CMMC: WHAT YOU NEED TO KNOW ABOUT DOD CYBERSECURITY REGULATION



EP#10 STUART ITKIN – EXOSTAR AND THEIR ROLE IN YOUR CMMC CERTIFICATION



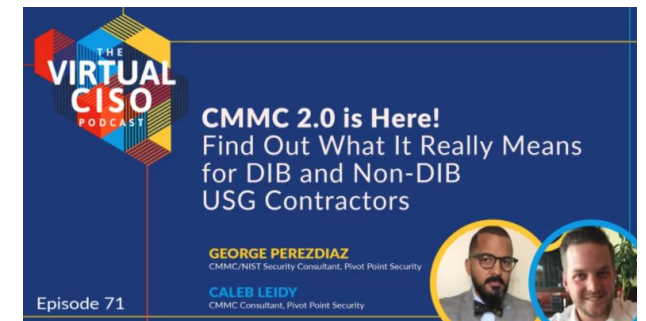
EP#22 BEN TCHOUBINEH – CMMC TRAINING & ASSESSMENTS: ROLLOUT, CERTIFICATION & COMPETITION



EP#21 SANJEEV VERMA – CMMC COMPLIANCE DOESN'T HAVE TO BE HARD (OR PRICEY)




EP#17 THOMAS PRICE – CMMC CERTIFICATION AUDITS - CAN YOU LEVERAGE ISO 27001?



EP#71 GEORGE PEREZDIAZ & CALEB LEIDY - CMMC 2.0 IS HERE!



**Any questions?
Reach out!**

 609-581-4600

 info@pivotpointsecurity.com