

Demystifying CMMC

December 10, 2024



CROSS TIMBERS
APEX Accelerator

PRESENTED BY: PHILLIP KNIGHT & GHASSAN KHATIB



Presenter Bios



Phillip Knight
Principal / Co-Founder

US: (888) 228-5620
UK: +44 20 7665 0408
D: (972) 910-2774
E: pknight@yesnovo.com
www.yesnovo.com

Phillip has a 25+ year career in technology development, integration and compliance management from small to large enterprises. He is a co-founder of NOVO who provides technology, cybersecurity and compliance services to small and mid-sized businesses.



Ghassan Khatib
Consultant Regulatory Affairs

US: (800) 625-4876
E: ghassan.khatib@tmac.org
www.tmac.org

Ghassan has a 25+ year career in developing and implementing management systems that serve the business objectives and meet regulatory requirements and applicable standards. His work covers enabling organizations for digital transformation and applying information technology. He is a business advisor in TMAC supporting companies in achieving compliance with CMMC, commonly through planning and implementing integrated systems and solutions that maintain regulatory and quality compliance and fulfill the controls of CMMC.



Shelia Birdow
PMP, ITIL, LSSGB, CEP
— BUSINESS DEVELOPMENT COORDINATOR

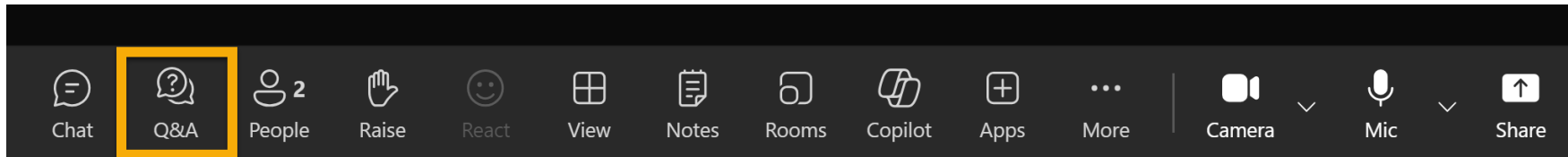
817-272-2081
Shelia.birdow@uta.edu
University of Texas Arlington
www.uta.edu/crosstimbers



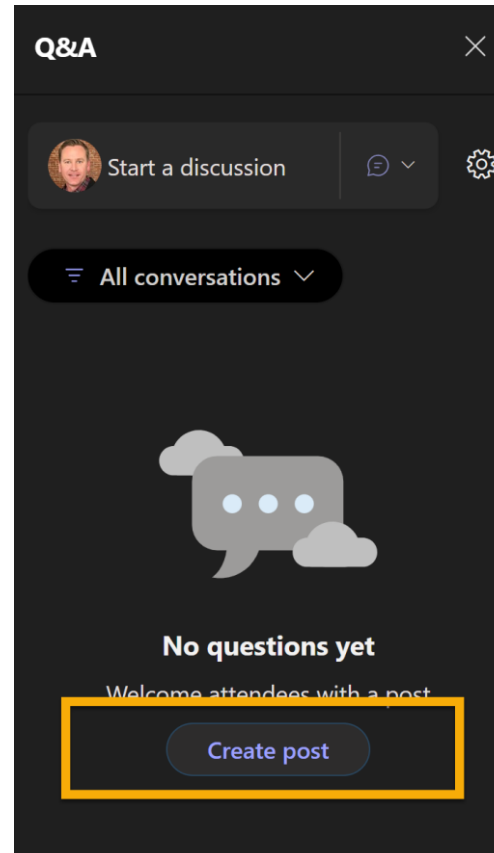
THIS APEX ACCELERATOR IS FUNDED IN PART THROUGH A COOPERATIVE AGREEMENT WITH THE DEPARTMENT OF DEFENSE.

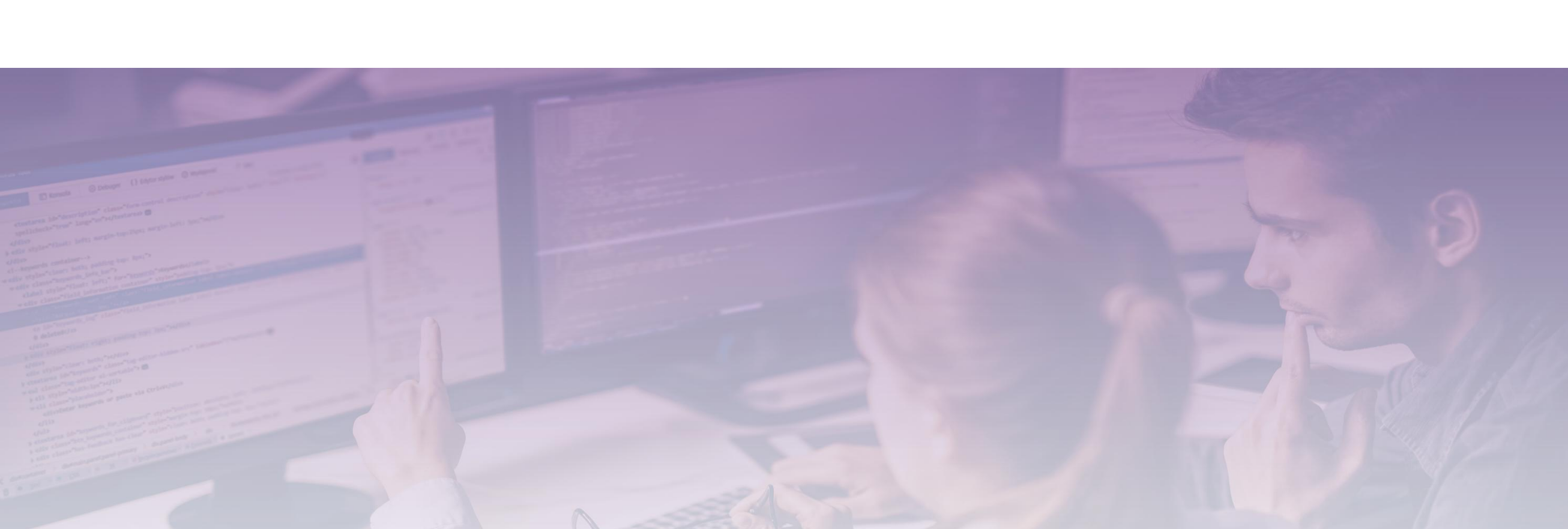
How to Ask a Question

1) Find the Q&A button in your Microsoft Teams toolbar



2) Create Post with your question.





The Fundamentals

CMMC OVERVIEW

Market Drivers for the U.S. Defense Industrial Base



\$800_B

Estimated 2024 DOD
spending in the U.S.
economy ¹

70%

Small-to-Mid size
business contribution to
Defense Industrial Base
(DIB) ²

30_k

Direct Small Defense
Industrial Base suppliers

1. [Center for Strategic & International Studies \(CSIS\)](#)

2. [Brookings](#)

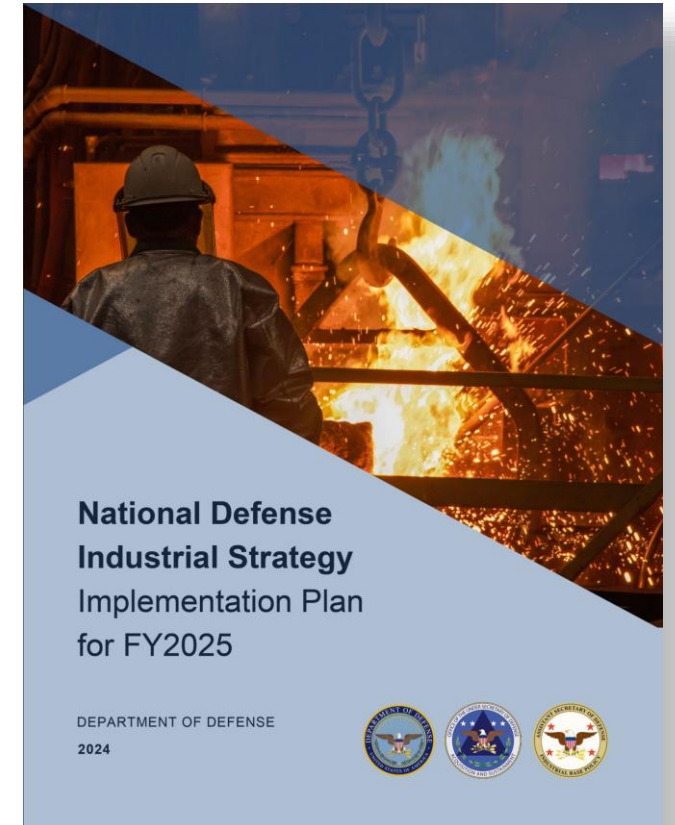
3. [Congressional Research Service](#)

Why CMMC?

*Numerous state and non-state actors have come to see cyberspace means as a powerful force multiplier. U.S. adversaries seek to use malicious cyber capabilities to achieve asymmetric advantages, targeting U.S. critical infrastructure, undermining U.S. economic security, and degrading U.S. military superiority. Hostile cyber-attacks pose an outsized danger to defense industry **intellectual property and supply chains**. Secure, reliable defense technology research and development and industrial base production is simply not possible without robust industrial cybersecurity.*

DoD CIO developed the Cybersecurity Maturity Model Certification (CMMC) program to reinforce the importance of defense industrial cybersecurity for safeguarding the information that support and enable our warfighters.

- Department of Defense



Key Protected Information Types

FEDERAL CONTRACT INFORMATION (FCI)

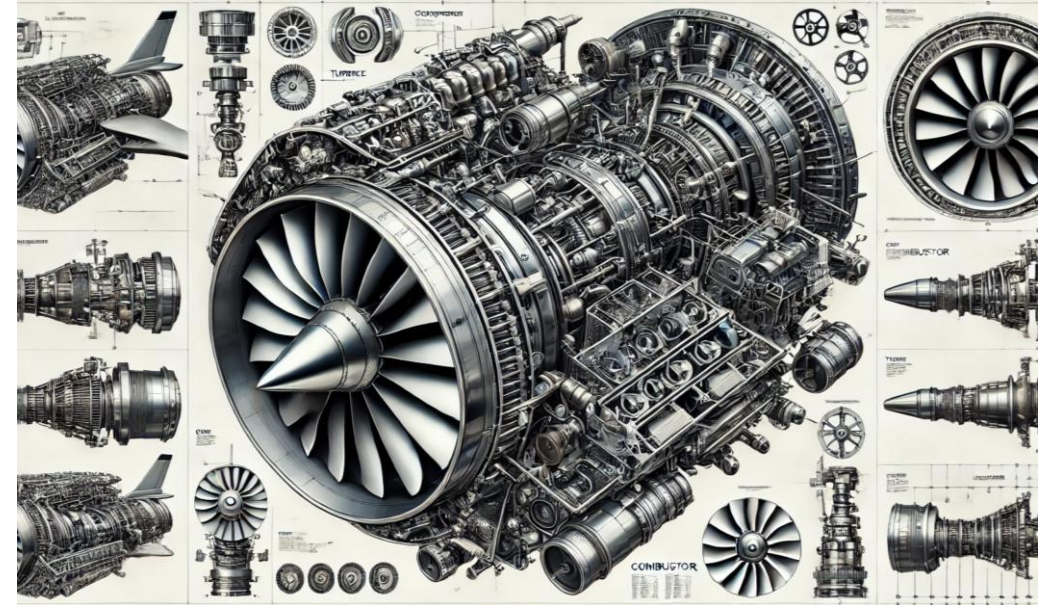
FCI is information, not intended for public release, provided by or generated for the government under a contract to develop or deliver a product or service to the government.



Federal Contract Information (FCI): is defined in FAR 52.204-21 and 48 CFR 4.1901 [3]

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

CUI is information that requires safeguarding for national security purposes according to laws, regulations, or government-wide policies but is not classified.



Controlled Unclassified Information (CUI): is defined in [32 CFR § 2002.4 \(h\) \[4\]](#)
More information available on the [CUI Registry](#)

FCI requires basic protection, generally covered by CMMC Level 1.

CUI is more sensitive, involving data that needs controlled access, requires CMMC Level 2 or higher protections.




What is CMMC?

Cybersecurity Maturity Model Certification (CMMC) is a framework created by the U.S. Department of Defense (DoD) to ensure that defense contractors implement and maintain adequate cybersecurity measures to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) within the Defense Industrial Base (DIB).

Aspect	Details
Purpose	Ensure DoD contractors have proper cybersecurity controls
Maturity Levels	Three (3) levels: Foundational, Advanced & Expert
Domains	14 Practice Areas (i.e. "Access Control", "Risk Assessment")
Key Frameworks Used	Based on NIST SP 800-171 r2 , with additional requirements
Assessment Type	Self-Assessment or third-party certification (contract dependent)
Certification Bodies	CMMC Third-Party Assessor Organizations (C3PAOs), DIBCAC
Applicability	Mandatory for all DoD contractors/subcontractors handling FCI or CUI

CMMC Compliance Level Requirements



CMMC Model	Model	Assessment	
<p>LEVEL 3</p>	<p>134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)</p>	<ul style="list-style-type: none"> • DIBCAC assessment every 3 years • Annual Affirmation 	<p>EXPERT (FCI & CUI) Must pass Level 2 audit with C3PAO prior to engaging DIBCAC for Level 3 audit.</p> 
<p>LEVEL 2</p>	<p>110 requirements aligned with NIST SP 800-171 r2</p>	<ul style="list-style-type: none"> • C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation 	<p>ADVANCED (FCI & CUI) Level 2 Self – Not critical to national security Level 2 C3PAO – Critical to national security</p>
<p>LEVEL 1</p>	<p>15 requirements aligned with FAR 52.204-21</p>	<ul style="list-style-type: none"> • Annual self-assessment • Annual Affirmation 	<p>FOUNDATIONAL (FCI only) No external audit required</p>

NIST SP 800-171 r2 Comparison with CMMC

Aspect	NIST SP 800-171 Rev. 2	CMMC
Purpose	Provides a set of security requirements for protecting CUI.	Certification framework for DoD contractors. Certifies compliance with cybersecurity practices.
Applicability	Mandatory for all federal contractors handling CUI under DFARS 252.204-7012.	Specifically designed for DoD contractors. CMMC builds upon NIST 800-171.
Structure	Contains 110 controls in 14 families (self-implemented).	Organized into 3 levels (CMMC 2.0), with varying control requirements.
Assessment Type	Self-assessment by the contractor (may include audits by the DoD).	Third-party assessments by C3PAOs for Level 2 and above.
Certification	No certification required; compliance is self-attested.	Certification required for CMMC compliance (Level 2 and above).
Focus	Security controls to meet DFARS requirements for safeguarding CUI.	Expands on NIST 800-171 with maturity and accountability.
Scope	Focuses on implementing security controls for systems handling CUI.	Includes system controls and organizational maturity (e.g., processes and practices).
Oversight	Adherence monitored primarily by the contractor; DoD may audit.	DoD requires certification by independent assessors (C3PAOs) for Level 2 & 3. In addition, DIBCAC/DoD assessment required for Level 3.
Integration	Used as the baseline for CMMC Level 2 controls.	Incorporates NIST SP 800-171 controls, with additional requirements.
Key Documents	System Security Plan (SSP), Plan of Action and Milestones (POA&M)	SSP, POA&M, plus evidence of process maturity.



CMMC goes beyond NIST SP 800-171, adding accountability, process maturity, and certification to ensure consistent implementation.



CMMC Control Scope



Business Management Controls

CA.L2-3.12.2
CA.L2-3.12.3
CA.L2-3.12.4
MA.L2-3.7.2
MA.L2-3.7.3
MA.L2-3.7.6
RA.L2-3.11.1

PROGRAM
{in-scope processes and applications needed for the contract}

Technology Controls

IA.L2-3.5.4
MA.L2-3.7.5
MP.L2-3.8.3
MP.L2-3.8.9
SC.L2-3.13.10
SC.L2-3.13.11
SC.L2-3.13.13
SC.L2-3.13.14
SC.L2-3.13.4
SC.L2-3.13.8

CM.L2-3.4.2
CM.L2-3.4.7
CM.L2-3.4.8
CM.L2-3.4.9
MP.L2-3.8.6
MP.L2-3.8.7
SC.L2-3.13.16

AC.L2-3.1.14
SC.L1-3.12.1

IA.L2-3.5.3
SI.L2-3.14.6

OPERATIONAL
{in-scope technology infrastructure and supporting services}

MA.2.111
MA.3.116
RE.3.130

AC.L1-3.1.1 AU.L2-3.3.1 IA.L2-3.5.6
AC.L1-3.1.2 AU.L2-3.3.2 IA.L2-3.5.7
AC.L2-3.1.10 AU.L2-3.3.4 IA.L2-3.5.8
AC.L2-3.1.11 AU.L2-3.3.7 IA.L2-3.5.9
AC.L2-3.1.15 AU.L2-3.3.8 SC.L1-3.13.5
AC.L2-3.1.16 AU.L2-3.3.9 SC.L2-3.13.12
AC.L2-3.1.17 CM.L2-3.4.6 SC.L2-3.13.15
AC.L2-3.1.18 IA.L1-3.5.1 SC.L2-3.13.3
AC.L2-3.1.4 IA.L1-3.5.2 SC.L2-3.13.6
AC.L2-3.1.5 IA.L2-3.5.10 SC.L2-3.13.7
AC.L2-3.1.7 IA.L2-3.5.11 SC.L2-3.13.9
AC.L2-3.1.8 IA.L2-2.5.5 SI.L1-3.14.4

AC.L2-3.1.13
AC.L2-3.1.19
AU.L2-3.3.6
RA.L2-3.11.2
SI.L1-3.14.2
SI.L1-3.14.5
SI.L1-3.14.7

STRATEGIC
{organization-wide secure practices}

Cyber Controls

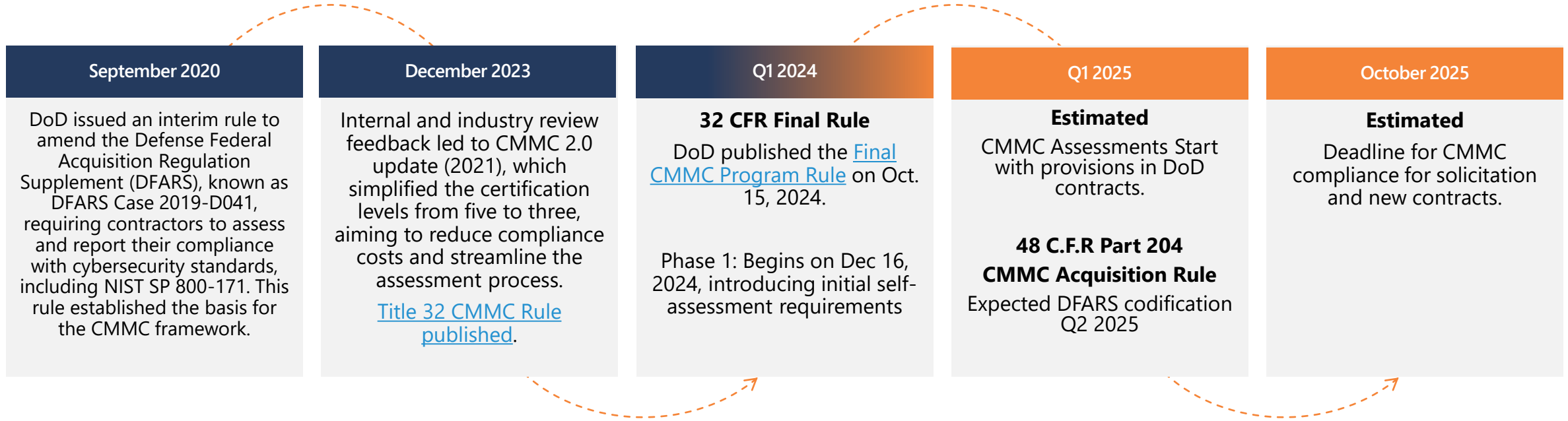
AC.L1-3.1.22 MP.L2-3.8.4
AC.L2-3.1.21 MP.L2-3.8.5
AC.L2-3.1.3 MP.L2-3.8.8
AC.L2-3.1.6 PE.L1-3-10-1
AC.L2-3.1.9 PE.L1-3-10-3
AT.L2-3.2.1 PE.L1-3-10-4
AT.L2-3.2.2 PE.L1-3-10-5
AT.L2-3.2.3 PE.L2-3-10-2
CM.L2-3.4.3 PE.L2-3-10-6
CM.L2-3.4.5 SP.L2-3.9.1
IR.L2-3.6.1 PS.L2-3.9.2
MP.L2-3.8.1 SI.L2-3.14.1
MP.L2-3.8.2

AC.L1-3.1.20
AC.L1-3.1.12
AU.L2-3.3.3
AU.L2-3.3.5
CA.L2-3.12.1
CM.L2-2.4.1
CM.L2-3.4.4
IR.L2-3.6.2
IR.L2-3.6.3
RA.L2-3.11.3
SC.L2-3.13.2
SI.L2-3.14.3

- Administrative (e.g. policies, standards & procedures)
- Assigned Tasks to Cybersecurity Personnel
- Technical Configurations (e.g. security settings)
- Assigned Tasks to IT Personnel
- Software Solution
- Assigned Tasks to Asset/Process Other
- Hardware Solution
- Configuration or Software Solution
- Software or Hardware Solution
- Configuration or Software or Hardware or Outsourced Solution



CMMC Key Events Timeline



CMMC Requirements Implementation



Organizations Need to Understand Attestation Risk



Self-attesting invalid or falsified information for CMMC compliance can pose significant risks to an organization, both legally and operationally.

Legal and Contractual Risks	Reputational Risks	Financial Risks	Cybersecurity Risks	Audits and Assessments	Loss of Certification
<ul style="list-style-type: none">• False Claims Act (FCA) Violations - \$27,000 per false claim• Contract Termination• Breach of Contract	<ul style="list-style-type: none">• Loss of Trust with Govt Agencies• Excluded Parties List System (Blacklisted)	<ul style="list-style-type: none">• Cost of Investigations• Lost Business Opportunities• Fines and Penalties (DFARS)	<ul style="list-style-type: none">• Increased Vulnerability• Liability for Breaches	<ul style="list-style-type: none">• DoD Audits• Increased Scrutiny	<ul style="list-style-type: none">• CMMC Certification Suspension or Revocation



The Department of Defense (DoD) takes cybersecurity compliance seriously to protect sensitive information. Providing inaccurate information can lead to severe consequences.



CMMC Accreditation Ecosystem



Registered Practitioner (RP)

Registered Practitioners are training and tested against the Levels based on the CMMC Framework to obtain their designation. They are implementers that are providing consultative preparation services to the Organizations Seeking Certification (OSC) and either work as independent contractors or as members of a Registered Practitioner Organization (RPO).



Registered Practitioner Organization (RPO)

A Registered Practitioner Organization (RPO) delivers a non-certified advisory service through the employment of RPs. They are consultative organizations or MSPs; and do not conduct Certified CMMC Assessments. Any references to “non-certified” services are only referring to the fact that an RPO is not authorized to conduct a certified CMMC assessment.



Certified CMMC Assessors (CCP/CCA)

A CCP is eligible to become CMMC Certified Assessor (CCA), participates up to CMMC Level 2 assessments, and holds a valuable credential reflecting the training to understand the CMMC requirements for a Defense supplier.



CMMC Third Party Assessment Organization (C3PAO)

A CMMC Third-Party Assessment Organization (C3PAO) conducts assessments of OSCs through the employment of CCPs and CCAs based on their rigorous training and adherence to CMMC standards.



Key Requirements Summary



- Self Assessments Begin in Phase I (Now)
- Level 1 (FARS) and Level 2 (NIST 800-171)
- Self Attestation Required as a stipulation of contract award.
- CYBER AB provides DIB accreditation
- Begin CUI Boundary Work
- Begin System Security Plan (SSP)

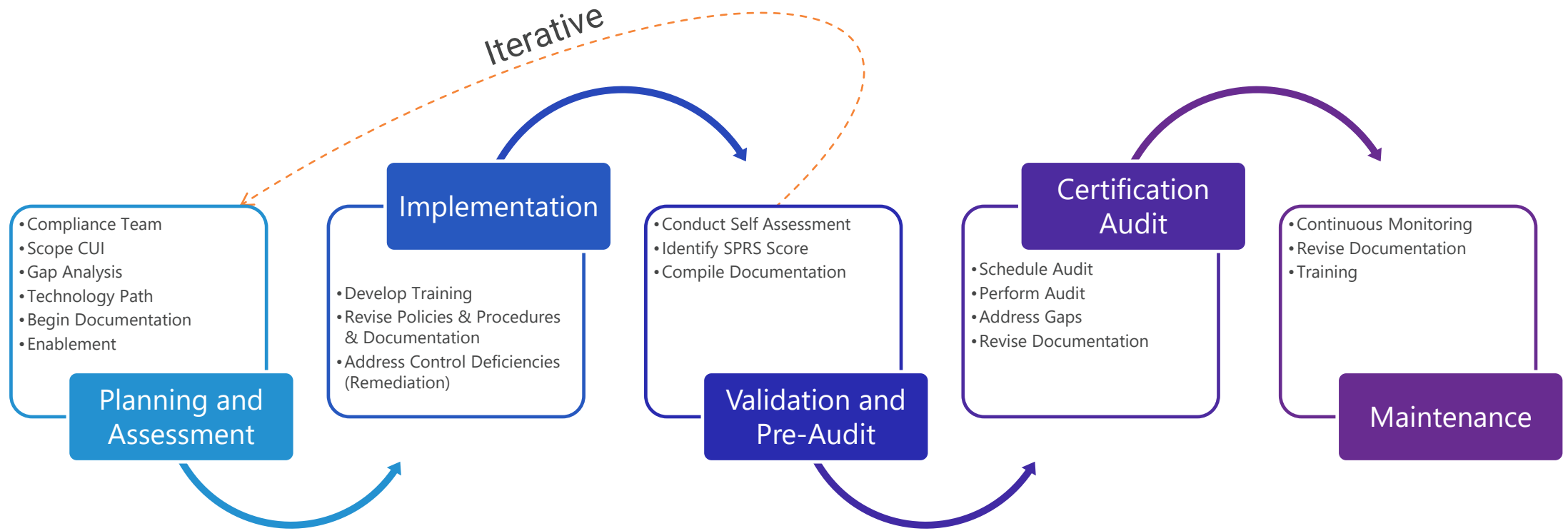


Achieving CMMC Compliance

The Journey Begins



Program Approach Designed to Manage Change



Skills
-Change Management -Process Management -Documentation & Training -Roles & Responsibilities -Communication

Decisions
-CMMC Level -3 rd Party Assistance -Technology Platform(s)

Tools
-Compliance Management Solution -Incident Management -Risk Register -Asset Management -CMMC Templates

Key Deliverables
-Policies & Procedures -System Security Plan (SSP) -Plan of Action & Milestones (POAM) -Customer Responsibility Matrix



NIST SP 800-171 r2 Control Families

Control Family	Description	Examples	Key Practices
Access Control (AC)	Limits access to systems and data to authorized users, processes, and devices.	- User role-based access - Multi-factor authentication	- Implement least privilege - Account management policies
Awareness and Training (AT)	Ensures personnel are trained to recognize and respond to security risks.	- Phishing training - Security awareness programs	- Conduct regular security training - Update policies based on emerging threats
Audit and Accountability (AU)	Tracks user activities and system changes to detect and respond to security incidents.	- Log files - SIEM (Security Information and Event Management)	- Enable logging for critical systems - Regular audit log reviews
Configuration Management (CM)	Establishes secure configurations for systems and prevents unauthorized changes.	- Use of baseline configurations - Version control	- Apply patch management - Review configurations regularly
Identification and Authentication (IA)	Verifies the identities of users and devices to prevent unauthorized access.	- Username and passwords - Biometrics	- Enforce password policies - Use secure authentication mechanisms
Incident Response (IR)	Prepares for, detects, and responds to security incidents effectively.	- Incident playbooks - Cyberattack drills	- Establish an incident response plan - Conduct post-incident reviews
Maintenance (MA)	Ensures systems are maintained securely and unauthorized maintenance is prevented.	- Regular hardware checks - Secure remote maintenance	- Document maintenance activities - Approve maintenance tools and methods
Media Protection (MP)	Protects digital and physical media containing sensitive information.	- Encrypt USB drives - Shred sensitive documents	- Label media properly - Use access-controlled storage areas
Personnel Security (PS)	Ensures personnel are vetted and understand their security responsibilities.	- Background checks - Termination procedures	- Define access control for personnel - Conduct regular evaluations
Physical Protection (PE)	Protects physical access to systems and information.	- Security guards - Locking server rooms	- Use surveillance cameras - Control visitor access
Risk Assessment (RA)	Identifies and assesses risks to the organization and its information.	- Risk matrix - Threat modeling	- Perform regular risk assessments - Update risk mitigation plans
Security Assessment (CA)	Evaluates the effectiveness of security controls and processes.	- Third-party audits - Penetration tests	- Conduct self-assessments - Maintain continuous monitoring
System and Communications Protection (SC)	Protects information during processing, storage, and transmission.	- Data encryption - Firewalls	- Use secure protocols (e.g., TLS) - Implement DLP (Data Loss Prevention) tools
System and Information Integrity (SI)	Detects and responds to information system vulnerabilities and incidents.	- Anti-malware tools - Vulnerability scans	- Apply security patches - Monitor for unauthorized changes



Many controls require continuous organizational capabilities and are not solely configuration



CMMC Level 1 - Foundational

Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1				IA.L1-3.5.1			MP.L1-3.8.3		PE.L1-3.10.1			SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2				IA.L1-3.5.2					PE.L1-3.10.3			SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20									PE.L1-3.10.4				SI.L1-3.14.4
AC.L1-3.1.22									PE.L1-3.10.5				SI.L1-3.14.5

FAR 52.204-21

Applies to Federal Contract Information (FCI), defined as information not intended for public release that is provided or generated for the federal government under a contract. Does not apply to classified information or Controlled Unclassified Information (CUI), which may require additional protections.



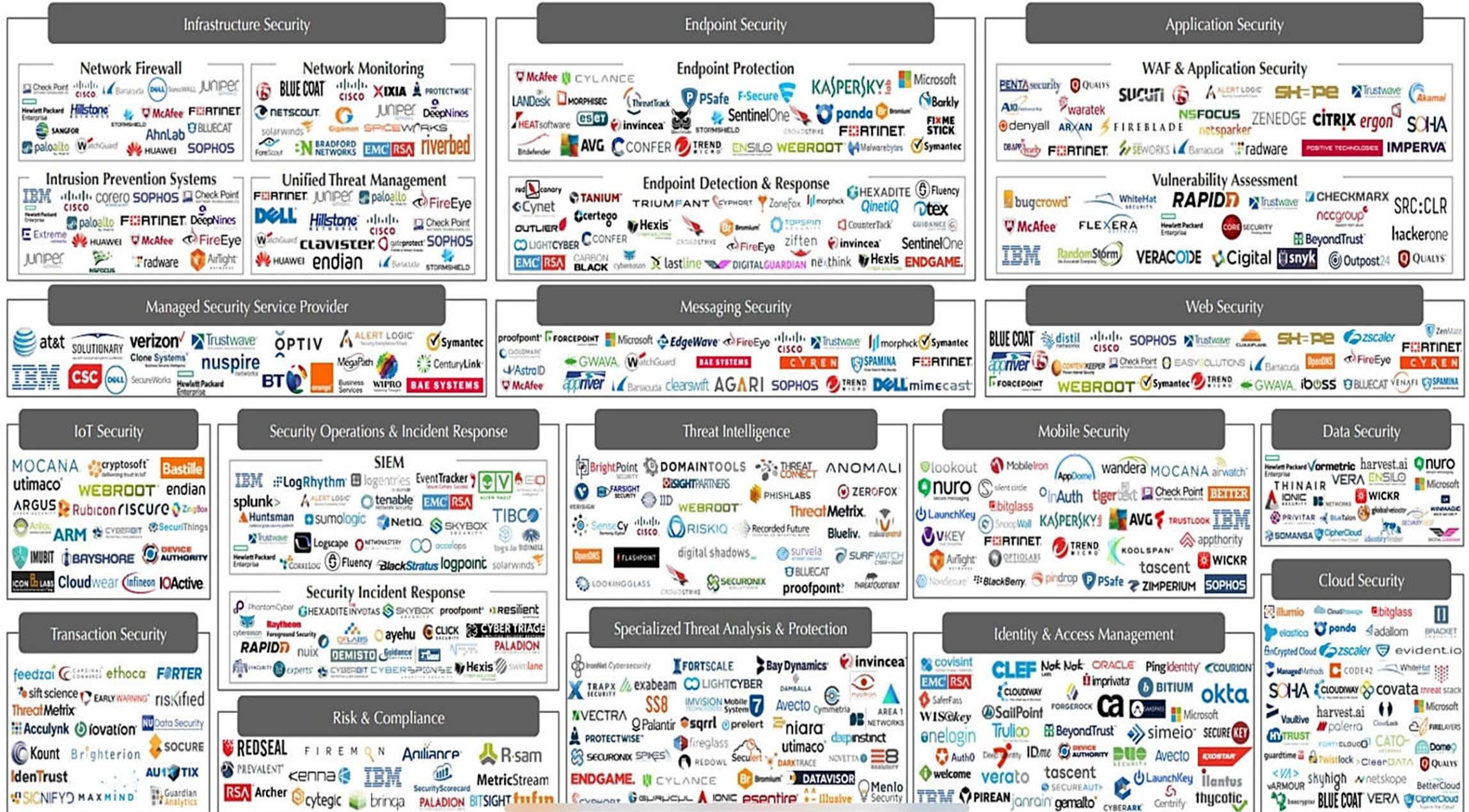
CMMC Level 2 - Advanced

Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.11.2	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.2	SI.L1-3.14.4
AC.L1-3.1.22	AU.L2-3.3.4		CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5		CA.L2-3.12.4	SC.L2-3.13.3	SI.L1-3.14.5
AC.L2-3.1.10	AU.L2-3.3.5		CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2			SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6			SC.L2-3.13.6	SI.L2-3.14.6
AC.L2-3.1.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.7	SI.L2-3.14.7
AC.L2-3.1.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.8	
AC.L2-3.1.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.9	
AC.L2-3.1.7				IA.L2-3.5.10								SC.L2-3.13.10	
AC.L2-3.1.8				IA.L2-3.5.11								SC.L2-3.13.11	
AC.L2-3.1.9												SC.L2-3.13.12	
AC.L2-3.1.11												SC.L2-3.13.13	
AC.L2-3.1.12												SC.L2-3.13.14	
AC.L2-3.1.13												SC.L2-3.13.15	
AC.L2-3.1.14												SC.L2-3.13.16	
AC.L2-3.1.15													
AC.L2-3.1.16													
AC.L2-3.1.17													
AC.L2-3.1.18													
AC.L2-3.1.19													
AC.L2-3.1.21													

CMMC Level 3 - Expert

Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.11.2	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.2	SI.L1-3.14.4
AC.L1-3.1.22	AU.L2-3.3.4	AT.L3-2	CM.L2-3.4.4	IA.L2-3.5.4	IR.L3-6	MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5	RA.L3-9	CA.L2-3.12.4	SC.L2-3.13.3	SI.L1-3.14.5
AC.L2-3.1.10	AU.L2-3.3.5	AT.L3-3	CM.L2-3.4.5	IA.L2-3.5.5	IR.L3-7	MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2	RA.L3-10	CA.L3-4	SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.3	AU.L2-3.3.6		CM.L2-3.4.6	IA.L2-3.5.6	IR.L3-8	MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6	RA.L3-11		SC.L2-3.13.6	SI.L2-3.14.6
AC.L2-3.1.4	AU.L2-3.3.7		CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.7	SI.L2-3.14.7
AC.L2-3.1.5	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.8	SI.L3-13
AC.L2-3.1.6	AU.L2-3.3.9		CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.9	SI.L3-14
AC.L2-3.1.7			CM.L3-3.4.8	IA.L2-3.5.10								SC.L2-3.13.10	
AC.L2-3.1.8			CM.L3-5	IA.L2-3.5.11								SC.L2-3.13.11	
AC.L2-3.1.9												SC.L2-3.13.12	
AC.L2-3.1.11												SC.L2-3.13.13	
AC.L2-3.1.12												SC.L2-3.13.14	
AC.L2-3.1.13												SC.L2-3.13.15	
AC.L2-3.1.14												SC.L2-3.13.16	
AC.L2-3.1.15												SC.L3-12	
AC.L2-3.1.16												SC.L3-3.13.2	
AC.L2-3.1.17													
AC.L2-3.1.18													
AC.L2-3.1.19													
AC.L2-3.1.21													
AC.L3-1													

The Cyber Security Tool Landscape



Technology Partner Differentiation

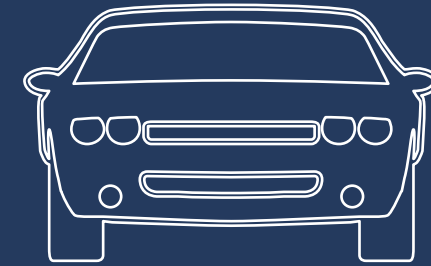
Compliance		Risk		MSP	CSP	MSSP	MDR	Recommended
ISO	NIST	Disaster Recovery	Infrastructure Management	✓				✓
			Network Management	✓				✓
Application Management			✓				✓	
Help Desk			✓	✓			✓	
CMMC			Infrastructure as a Service (IaaS)		✓			✓
			Software as a Service (SaaS)		✓			✓
			Platform as a Service (PaaS)		✓			✓
			Security Management	✓	✓	✓	✓	✓
			Intrusion Detection			✓	✓	✓
			Firewall Management			✓		✓
	Vulnerability Scanning			✓		✓		
	Continuous Monitoring			✓	✓	✓		
	Threat Intelligence			✓	✓	✓		
	Incident Response				✓	✓		
Exfiltration of Data	Real-time Threat Detection				✓	✓		
	Rapid Incident Response				✓	✓		
	Advanced Analytics				✓	✓		
	Proactive Support	✓				✓		
	Ransomware	Scalability Solutions			✓		✓	
		Accessibility Solutions			✓		✓	
		IT Consulting	✓	✓			✓	



CMMC Technology Pathways



Typical CMMC Strategy



“One Stop Shop”



Unified Compliance Strategy

First Steps Toward Certification



- Get educated & begin stakeholder awareness

- Determine required CMMC level

- Consolidate technology and solution vendors and ensure they meet CMMC compliance.

- Conduct a self-assessment ([link](#))

- Begin CUI Boundary Work

- Begin System Security Plan (SSP)

Next Steps

yesnovo.com/cmmc

[Schedule Free CMMC Consultation](#)





Question & Answer