WEBINAR

CMMC: An Introduction

June 1, 2021

ankura

ankura.com

AGENDA

ANKURA COMPANY PROFILE (12:00-12:15)

CMMC OVERVIEW (12:15-12:30)

CMMC REQUIREMENTS (12:30-12:55)

CMMC ECOSYSTEM (12:55-1:05)

ASSESSMENTS (1:05-1:15)

CLOSING AND Q&A (1:15-1:30)

ankura

Presenters

Alan Levesque

Senior Managing Director
National Security, Trade & Technology

- JD with over 30 years as a U.S. Army Officer, senior C-suite ethics & compliance executive, practicing litigation attorney, in-house legal counsel, and compliance professional.
- Former vice president and compliance leader at two international high technology companies, with significant U.S. Government business lines.
- Widely respected in the industry and amongst regulators as an effective change agent to drive compliance and operational improvement.

Joe Moyer

Senior Director
National Security, Trade & Technology

- JD with 15 years of experience as a U.S. Navy JAG and management consultant.
- Provided range of compliance and risk consulting services to companies within the aerospace & defense sector; focus on alignment of operations and compliance functions
- Holder of Project Management Professional (PMP) and Certified Fraud Examiner (CFE) certifications; Executive Master's in Leadership from Georgetown University

Gary Espinoza

Senior Director
National Security, Trade & Technology

- IT Professional with 20+ years' experience in aerospace and financial services at Fortune 100 companies
- Extensive experience assessing and integrating ITAR controls into IT systems and infrastructure
- MBA in Finance from Fordham University
- Certified AWS Solution Architect Associate

Alex Trafton

Director
National Security, Trade & Technology

- 10 years of experience as a risk management leader with a focus in information security, program development, and compliance.
- Has led multiple engagements assessing organizational cybersecurity programs against the NIST 800-171 and CMMC frameworks.
- CMMC-AB Registered Practitioner, ISO 27001 Foundation, Certificate in Cybersecurity Management – Harvard University.

Who we are

Ankura is a full-service professional services firm of **over 1,500 professionals** with locations in over **30 major cities** throughout the world.

We tailor our approach to each client's unique needs, combining subject matter expertise, industry experience, government and regulatory perspective, technical skills, proprietary tools, and cutting-edge technology to deliver comprehensive, practical, and cost-effective solutions.

Services Overview

ANALYTICS & DIGITAL TRANSFORMATION

- Analytics and Data Strategy
- eDiscovery
- MDL*Online*
- Technology Advisory

CYBERSECURITY

- **CISO and Cybersecurity Leadership Services**
- Compromise Detection
- Cyber Investigations
- Cybersecurity and Privacy Compliance
- **Cybersecurity Assessments and Audits**
- Cybersecurity Strategy, Policy, and Maturity
- Data Governance
- Data Privacy and Regulatory Compliance
- Incident Response
- Network, Web, and Mobile Application Security
- Response Preparedness
- Third Party Cyber Due Diligence
- Threat and Vulnerability Evaluation and Remediation

ECONOMICS & STATISTICS

- Class Action/Class Certification
- Intellectual Property Litigation Economic Damages
- Labor and Employment
- Statistical Analysis, Econometrics and Data Analytics
- Regulatory Disputes

INTELLECTUAL PROPERTY

- Intellectual Property Management and Monetization
- Litigation Support and Expert Services
- Royalty Analysis and Disputes
- Valuation Consulting
- Fair, Reasonable, and Nondiscriminatory (FRAND)

INVESTIGATIONS & ACCOUNTING ADVISORY

- Anti-Corruption
- AML
- Audit Advisory
- Cryptocurrency and Blockchain Advisory
- Forensic Accounting and Financial Investigations
- Investigations
- Regulatory Accounting and Technical Advisory
- White Collar and Securities

LITIGATION, ARBITRATION, & DISPUTES

- Antitrust and Competition
- Commercial Disputes
- Damages Analysis
- Economics and Statistical Analysis
- Bankruptcy Litigation
- Expert Services
- Intellectual Property
- International Arbitration
- Mass Torts and Class Actions
- Purchase Price Disputes
- Royalty Analysis and Disputes
- Tax Controversy
- Visual Communications

RISK MANAGEMENT & COMPLIANCE ADVISORY

- Compliance and Ethics
- Crisis Preparedness and Operational Resilience
- Government Contracts and Grants
- **National Security, Trade, & Technology**
- Monitoring and Independent Oversight

STRATEGY & PERFORMANCE

- *Advanced Human Capital*™
- Growth Advisory
- Merger and Acquisition Performance
- Performance Optimization
- Program and Change Management
- Strategic Planning

TRANSACTION ADVISORY SERVICES

- Business and Ownership Interest Valuation
- Financial Reporting Valuation
- Foreign Investments Advisory
- Merger and Acquisition Performance
- Property Insurance Valuation

TURNAROUND & RESTRUCTURING

- Bankruptcy Services
- Chief Restructuring Officer
- Company Restructuring Advisory
- Geopolitical Intelligence
- Interim Management
- Lender Restructuring Advisory

NSTT Practice

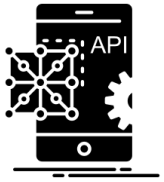
Ankura's NSTT Team offers an interdisciplinary array of national security-oriented capabilities to help companies, investors, and counsel navigate a changing policy and regulatory environment:

Foreign Investment and Control	Int'l Trade Controls	CMMC / Cyber-security	Supply Chain	Federal Subsidiary Solutions
• CFIUS • Transaction Risk • Third Party Oversight • Team Telecom • Trust Vehicles	• Export • Import • Sanctions	• Assessments • Enhancements • Secure Solutions • Certification Prep	• Diligence • Product Integrity • SCRM	• FOCI/FCL • DARPA • OPSEC • Cleared Programs

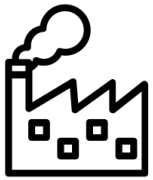
To learn more please visit the Ankura National Security, Trade and Technology website.

CMMC | Past Performance, Deep Experience

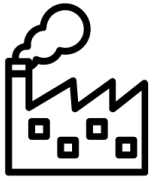
1. Ankura was engaged by a mid-sized U.S. Aerospace company to assess and enhance is cybersecurity program in preparation for achieving the CMMC Level 3 certification and to provide advisory services for a technology separation plan and framework for the company's anticipated spinoff transaction. Ankura reviewed the company's existing policies and procedures and interviewed key cybersecurity personnel to provide a thorough assessment of the company's CMMC Level 3 posture and identified areas of enhancement for the company to consider in order to meet CMMC Level 3 requirements.



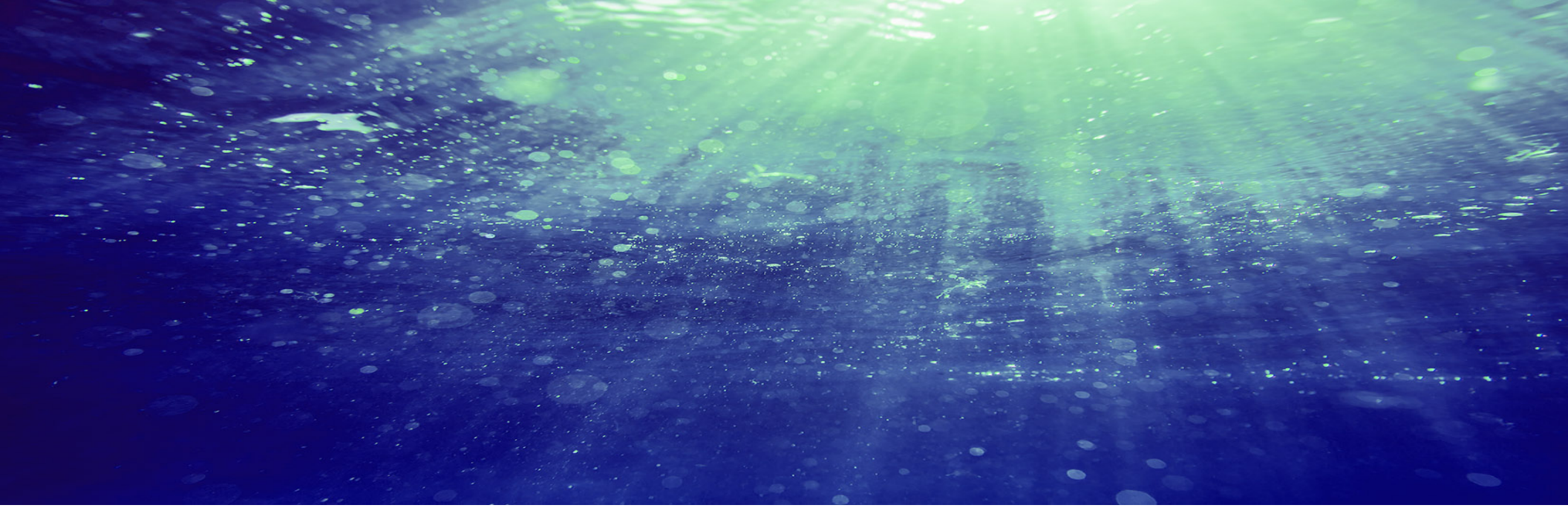
2. Ankura was engaged by a U.S. based software company to provide advisory and assessment services to help prepare the company's enterprise environment and systems for achieving the CMMC Level 3 certification. Ankura team members reviewed and mapped the company's policies and procedures to the NIST 800-171 and CMMC requirements in a System Security Plan.



3. Ankura is engaged by a U.S. based metal manufacturing company to assess the 130 security controls of the CMMC Level 3 in its regulated data environment. Ankura also conducted a risk assessment in the company's regulated data environment in fulfillment of the CMMC control RM.2.141.



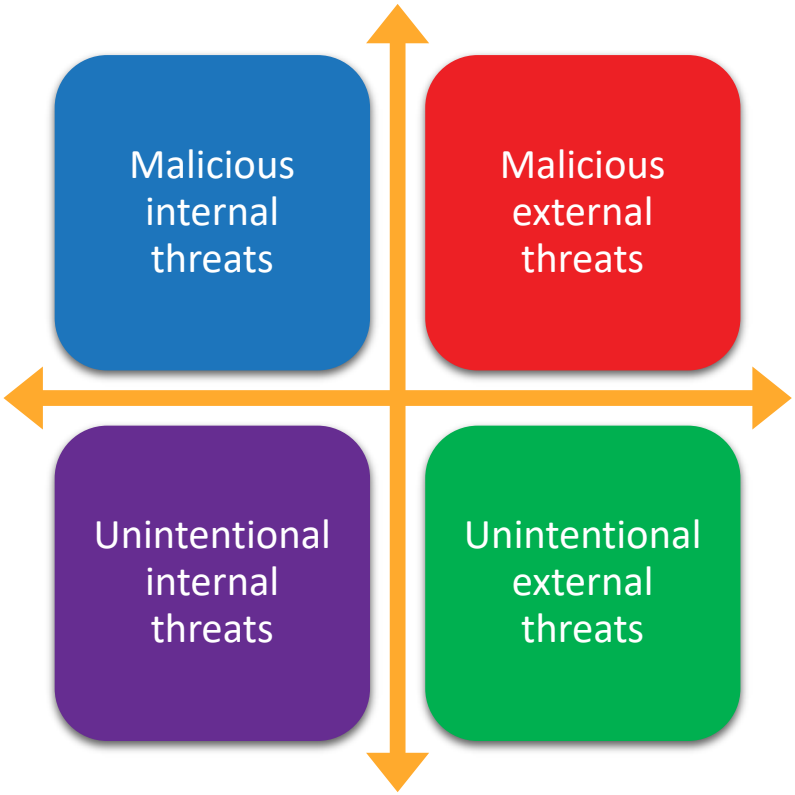
4. Ankura was engaged by a foreign manufacturing company to assess its current state cybersecurity posture against both ISO 27001 and NIST 800-171. Ankura provided a risk assessment and submitted a 230-page detailed report, presented a substantial remediation and maturity roadmap, plan, and timeline, which the company has budgeted for FY 2021 to support cybersecurity requirements to enter the defense supply chain.



CMMC: Overview

ankura

Cybersecurity| Classifying Threat Types



Advanced Persistent Threats

Cyber Criminals

Insider Threats

Confidentiality

Integrity

Availability

Cybersecurity Ventures predicts that cybercrime will cost the world economy $6 trillion in 2021. That number rises to $10.5 trillion by 2025.

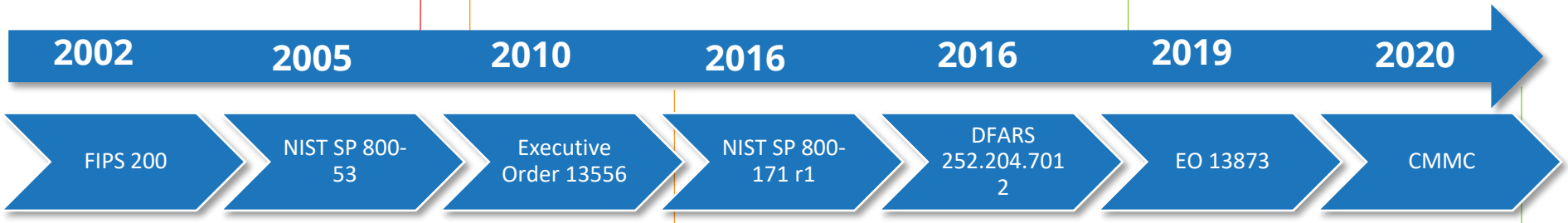
CMMC | Origins to Present

The CMMC is the culmination of almost two decades of cumulative cybersecurity models that have evolved with the increasing maturity of threat actors and attack vectors.

2007 - USG suffers massive cyber attack in which an unknown foreign power broke into the high-tech agencies, all military agencies, and downloaded terabytes of information

2009 - Operation Aurora was launched by China against Google and over 20 other companies.

2018 - DoJ charges nine Iranians with stealing scientific secrets on behalf of Iran's Revolutionary Guard Corps. These individuals stole 31TB of data from public and private organizations.



2013-15 OPM breach: Millions of personnel records compromised, including SF-86 forms, fingerprints, and other critical PII

SolarWinds: Orion network management tool was deployed to approx. 18,000 customers, including federal agencies, and with it, malware which compromised an untold amount of USG and private sector data.

CMMC | Past, Present, & Future

Moving from a self-attestation model to a fully validated and audited cybersecurity model will take time. The DoD understands that this is a multi-year approach and has created expectations that allow for a growing maturity across the 300,000 contractors in the Defense Industrial Base (DIB).

Pre-CMMC Environment

Contractors *handling CUI* self-attested to compliance with NIST 800-171 under DFARS 252.204.7012

Pre-2020

Staggered CMMC Rollout

1. Self attestation to NIST 800-171 at 3 levels of assurance, with each DoD contract renewal and new procurement that specifies DFARS 7012 – No CMMC Required.

2. DFARS and CMMC obligations continue side by side.

3. CMMC becomes adopted by GIS for federal civilian procurements.

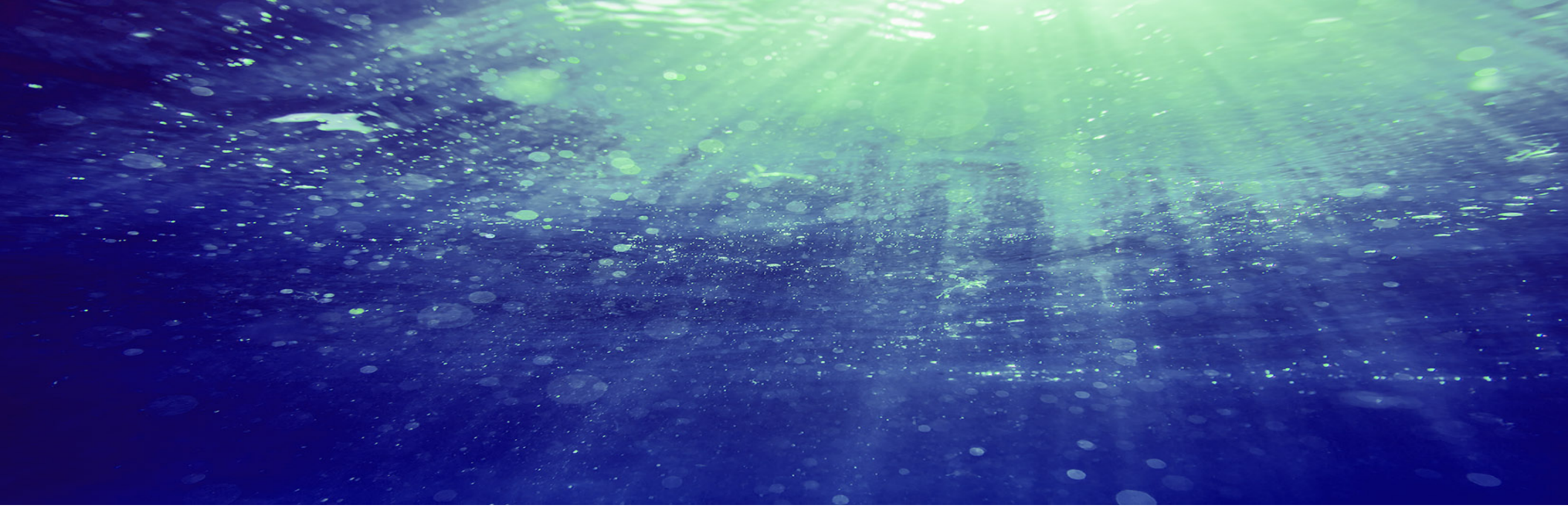
November 2020 to October 2025

Full Deployment of CMMC

1. All DoD procurements require binary 3rd party CMMC audit.

2. Passed DIBCAC audits of NIST 800-171 have reciprocity with CMMC.

October 2025 Forward

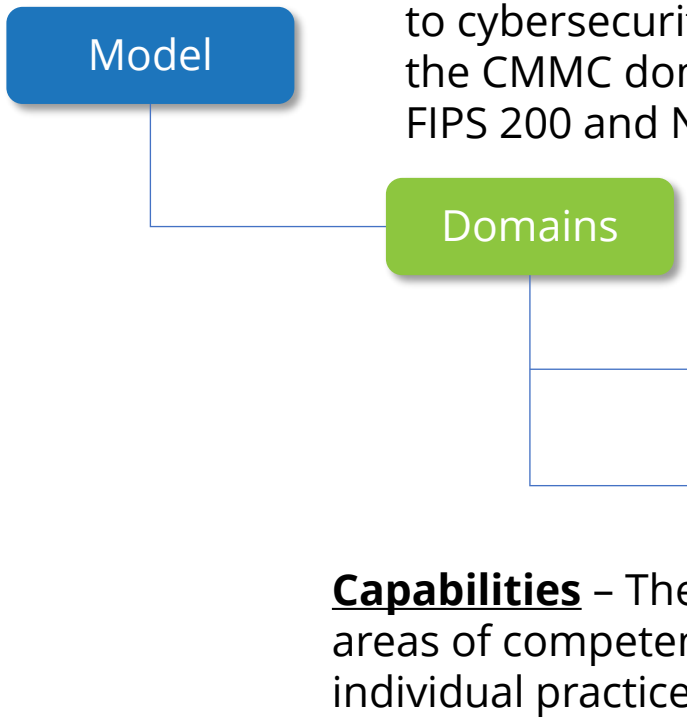


CMMC: Requirements

ankura

CMMC| Key Terms

CMMC has a unique terms that an entity working either as a prime or a sub to obtain CMMC accreditation should understand.



Domain – Broad areas relating to cybersecurity, the majority of the CMMC domains originate in FIPS 200 and NIST SP 800-171.

Processes – The adoption of processes across the 17 domains of the CMMC demonstrate the level of institutionalization of the individual required practices.

Processes

For a given domain, there are processes that span a subset of the 5 levels

Capabilities

For a given domain, there are one or more capabilities that span a subset of the 5 levels

Capabilities – The specific areas of competency that individual practices will demonstrate in each domain.

Practices

For a given capability there are one or more practices that span a subset of the 5 levels

Practices – The specific, individual controls to be implemented to achieve the desired level of cybersecurity maturity.

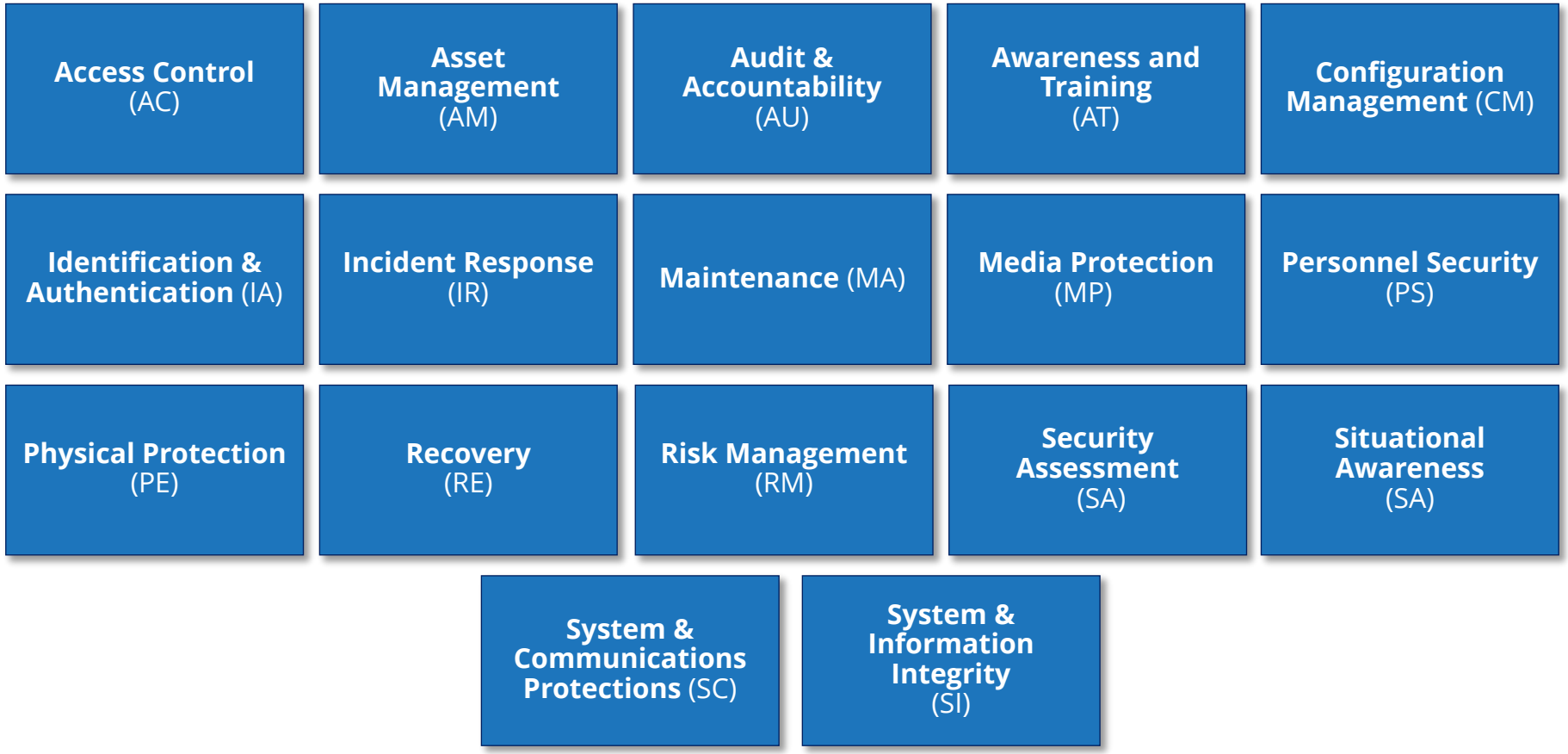
The Maturity Model | What's Included

Each level of CMMC contains a series of escalating requirements. Of note, the same contract may require different certification levels depending on contractual responsibilities and tasks assigned to the prime and the sub.

Level 5	110 security requirements from NIST SP 800-171 + 61 CMMC practices + 5 CMMC processes = 171 Practices + 5 Processes
Level 4	110 security requirements from NIST SP 800-171 + 46 CMMC practices + 4 CMMC processes = 156 CMMC Practices + 4 Processes
Level 3	110 security requirements from NIST SP 800-171 + 20 CMMC practices + 3 CMMC processes = 130 Practices + 3 Processes
Level 2	65 security requirements from NIST SP 800-171 + 7 CMMC practices, and 2 CMMC processes = 72 CMMC Practices + 2 Processes
Level 1	15 basic requirements (FAR clause 52.204-21) = 17 CMMC Practices

CMMC Domains | Building Best Practices

The CMMC consists of 17 domains. The majority of these domains originate from the security related areas of the Federal Information Processing Standards (FIPS) publication 200 [2002] and the related security requirement families from NIST SP 800-171 [2016]. The CMMC model also includes the three domains of Asset Management (AM), Recovery (RE), and Situational Awareness (SA).



What are the Processes?

1. **Level 2 Process**: Establish a policy that includes [Domain Name].
2. **Level 2 Process**: Document the CMMC practices to implement the [Domain Name] policy.
3. **Level 3 Process**: Establish, maintain, and resource a plan that includes [Domain Name].

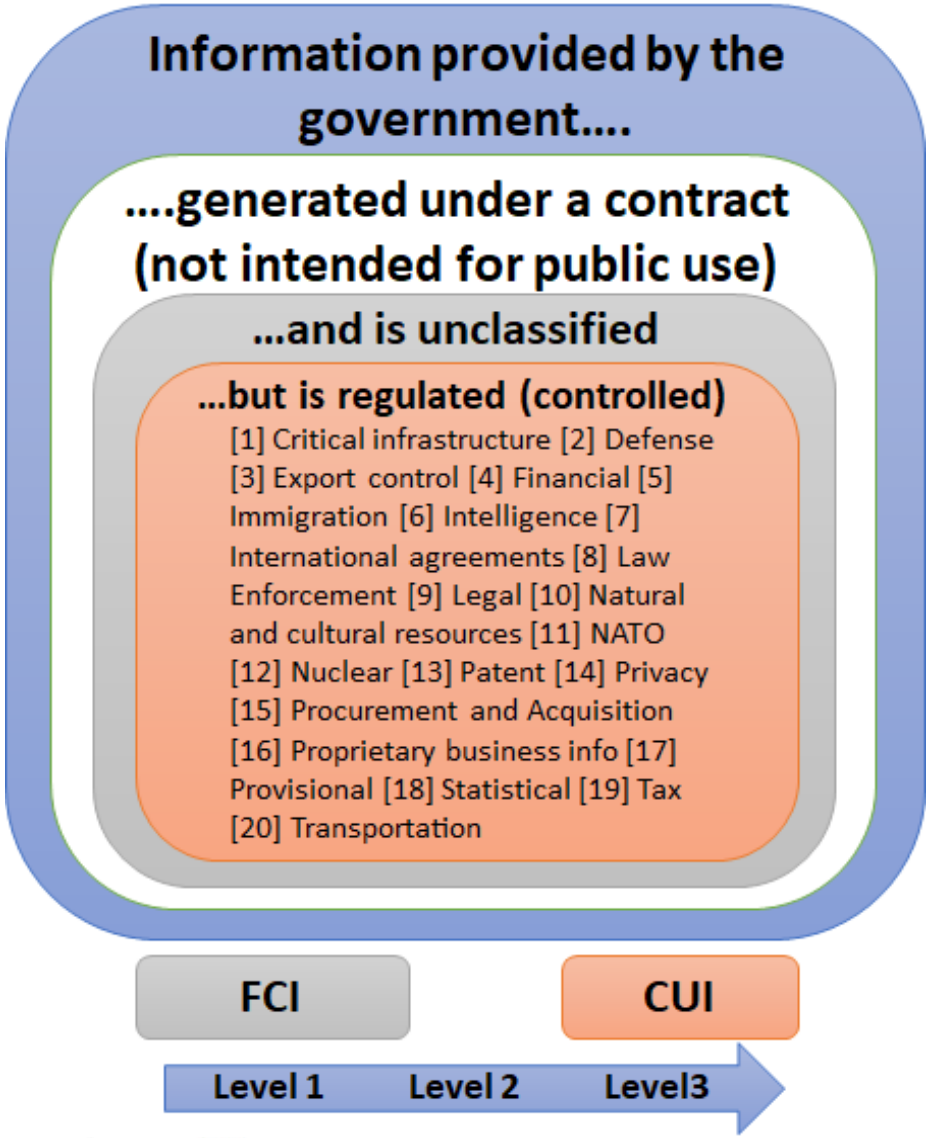
What is the Assessment Standard?

Two forms of objective evidence from:

Specifications: Document-based artifacts.
Mechanisms: Specific hardware, software, or firmware.
Activities: Protection-related actions supporting a system that involve people.
Individuals or groups of individuals: People applying the specifications, mechanisms, or activities described above.

CMMC| Key Terms

CMMC has a unique terms that an entity working either as a prime or a sub to obtain CMMC accreditation should understand.



Federal Contract Information (FCI) – *"Information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public…"*
-FAR clause 52.204-21

Controlled Unclassified Information (CUI) – *"Information the Government creates or possesses, or that an entity creates or possesses on for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."*
[CUI excludes classified information]
-Established by EO 13556

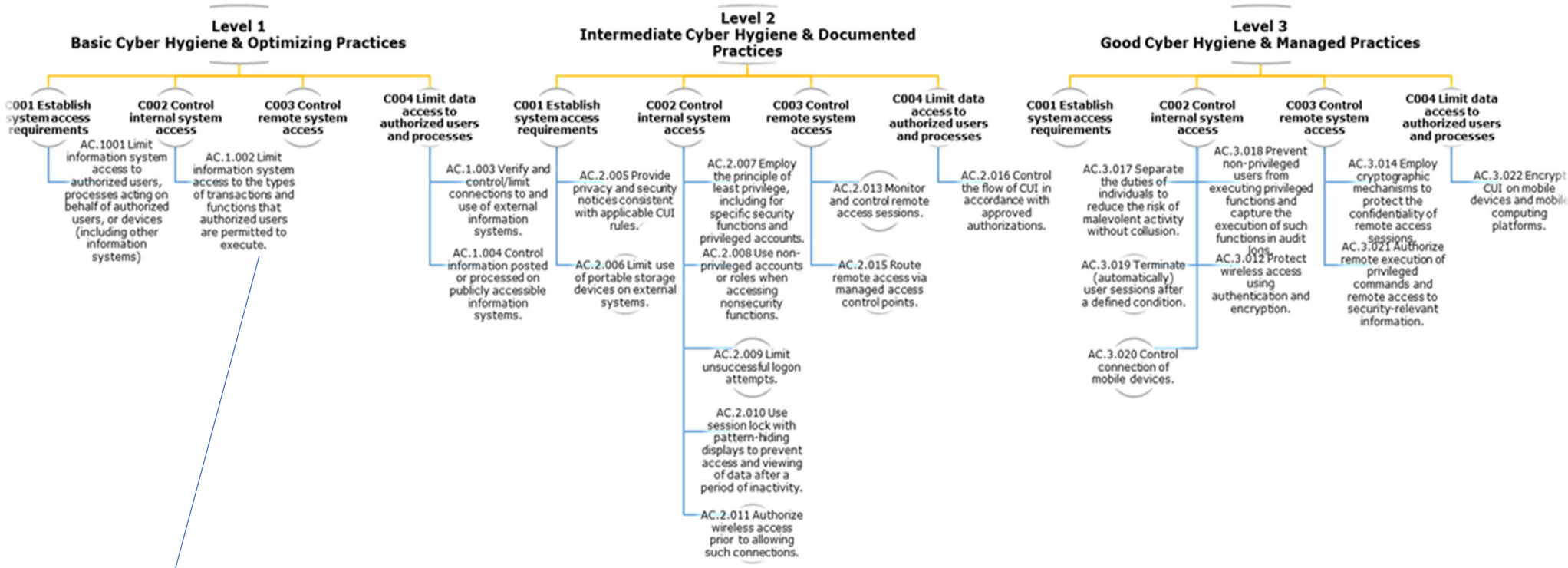
What are Capabilities?

Each domain has an associated set of capabilities. There are 43 defined capabilities spanning the 17 CMMC domains.

Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Audit & Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Identification & Authentication (IA)	• Grant access to authenticated entities

All controls within these domains will relate to the capabilities established in the CMMC framework.

Access Control (AC)



AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

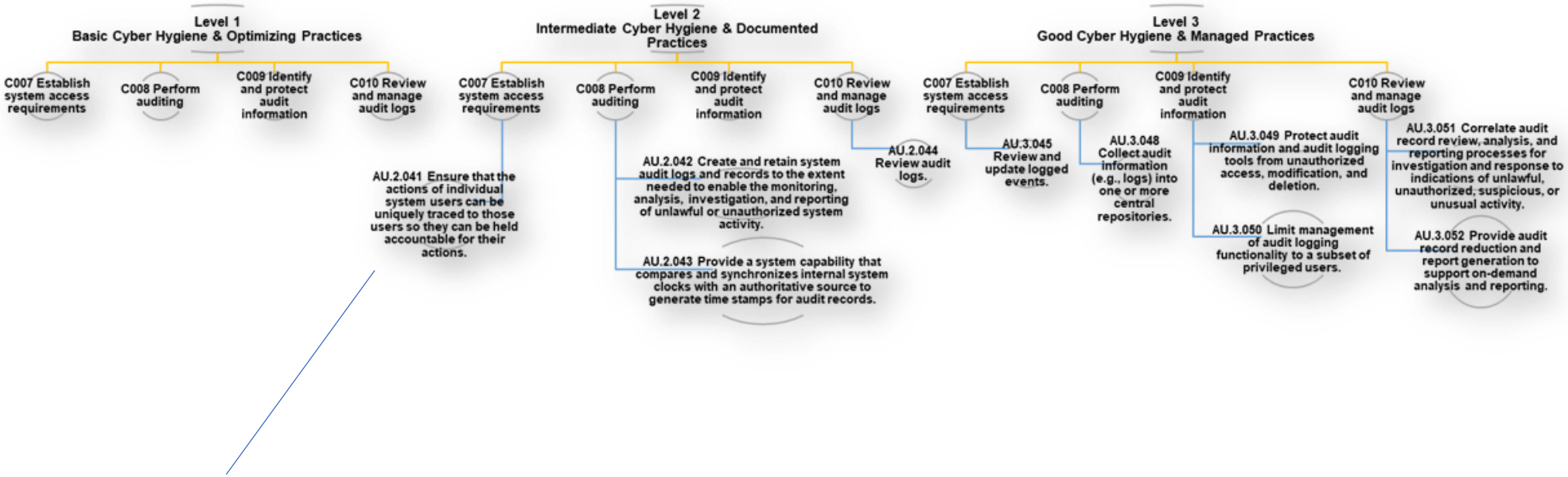
Assessment Objectives

Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[b] system access is limited to the defined types of transactions and functions for authorized users.

Audit & Accountability (AU)



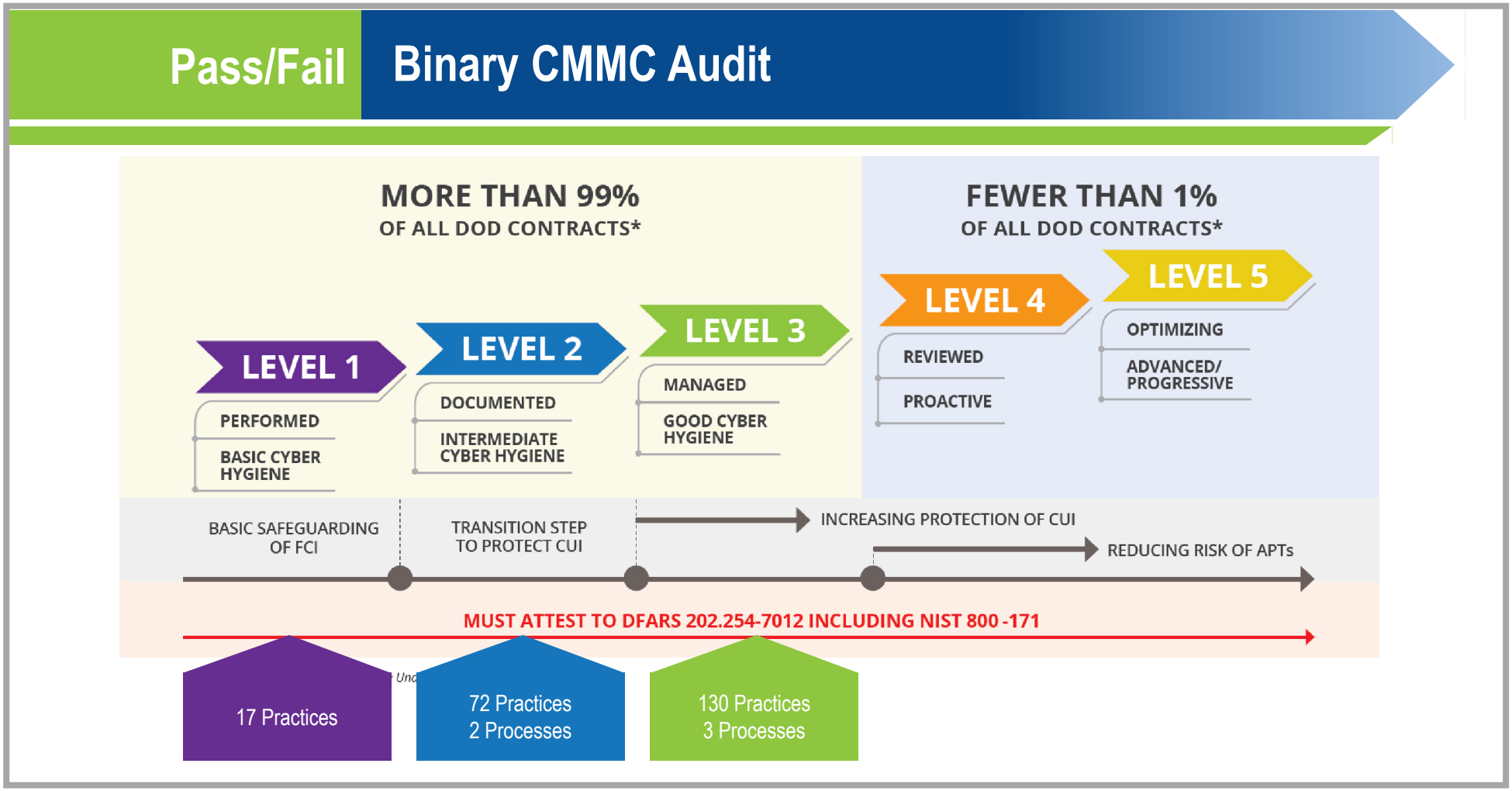
AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions

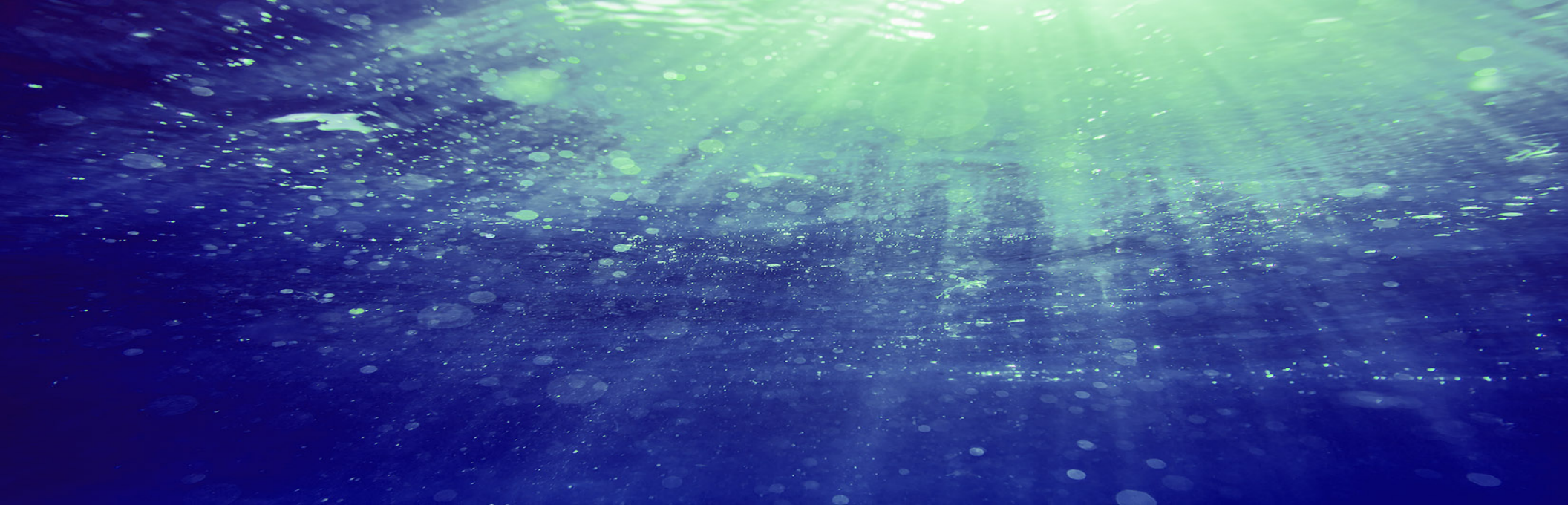
Assessment Objectives

Determine if: [a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and [b] audit records, once created, contain the defined content

CMMC | Binary Process

While the CMMC is a pass/fail audit, companies are not expected to be able to pass a high-level audit right away. Most of the in-scope controls for Level 3 are the 110 controls in the NIST SP 800-171 and are already required under DFARS 202.254.7012.



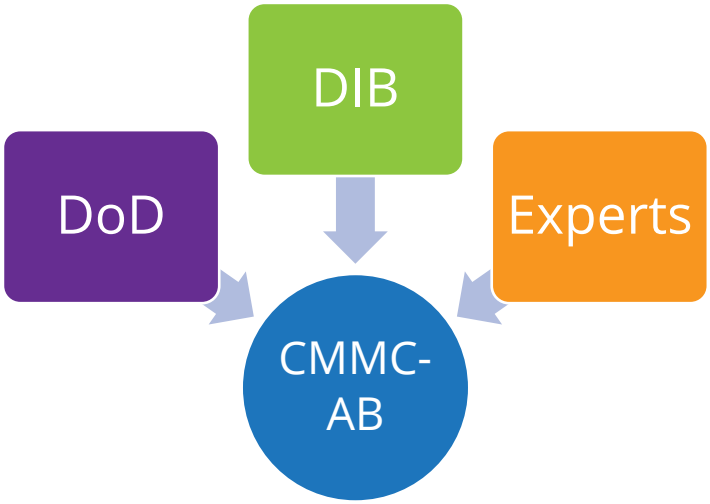


CMMC: Ecosystem

ankura

CMMC | A Public-Private Partnership

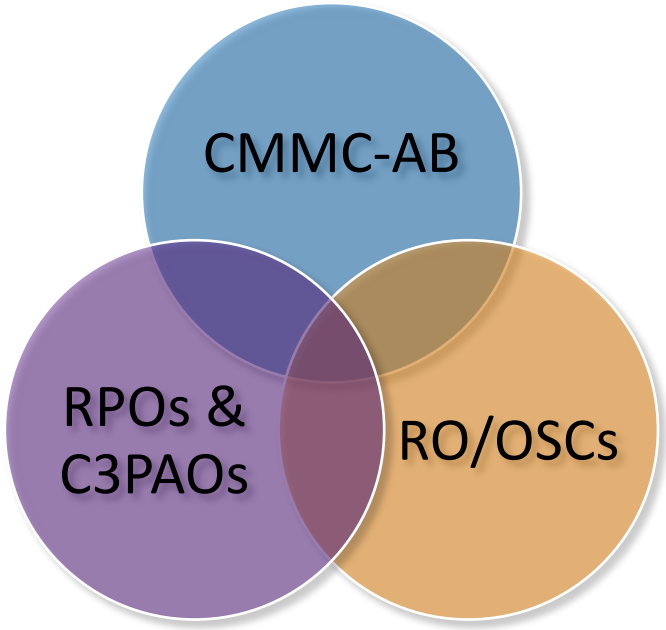
- While the CMMC is a cybersecurity mandate from the DoD, the DoD understands that the best, most well-resourced solution will come from the private sector.
- The DoD has established the CMMC Accreditation Body (CMMC-AB) which is a private sector, non-profit governing body that will create and maintain the CMMC ecosystem.
- The CMMC-AB will set the training standards for private sector consultants and auditors to manage the advising and auditing process for organizations seeking certification.
- This ecosystem will create a competitive market assuring that services are delivered in a cost-efficient manner, while maintaining the professional standards and intent set by the DoD.



"We must elevate cybersecurity as an imperative across the government in order to defend the American people and U.S. critical infrastructure. Additionally, the government must continue to strengthen its partnership with the private sector to foster greater information sharing and collaboration."

Lloyd Austin, Army General (Ret.) during his Senate confirmation hearing for Secretary of Defense.

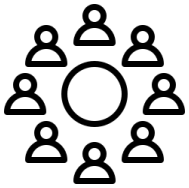
CMMC Ecosystem | Consulting & Auditing



The CMMC-AB will also oversee an ecosystem of training providers and content publishers. These entities will have the responsibility of developing and delivering approved content and courses to organizations and individuals seeking to enter the ecosystem as consultants and assessors. The CMMC-AB is ultimately a licensing entity that oversees the curriculum and code of conduct for the CMMC.

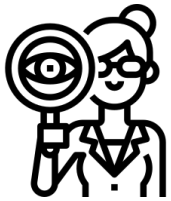
Reliant Organizations: Prime contractors who will be required to flow down CMMC requirements/certification.

Organizations Seeking Certification (OSC): Subcontractors in the supply chain who will be required to demonstrate compliance.



CMMC-AB: A non-profit organization managing the CMMC Ecosystem and issuing certification OSCs.

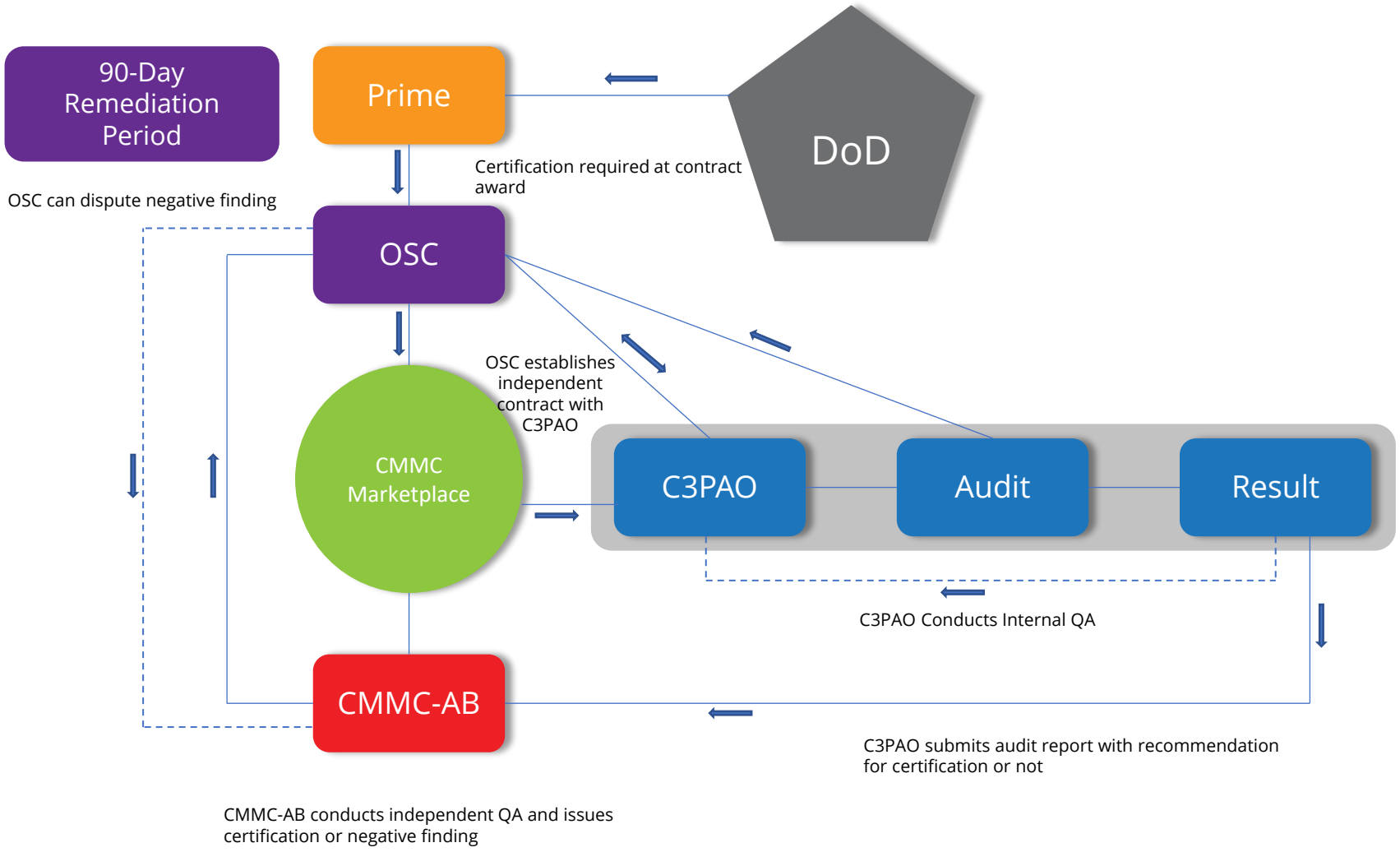
Registered Provider Organizations (RPOs): Approved organizations providing CMMC consulting services.

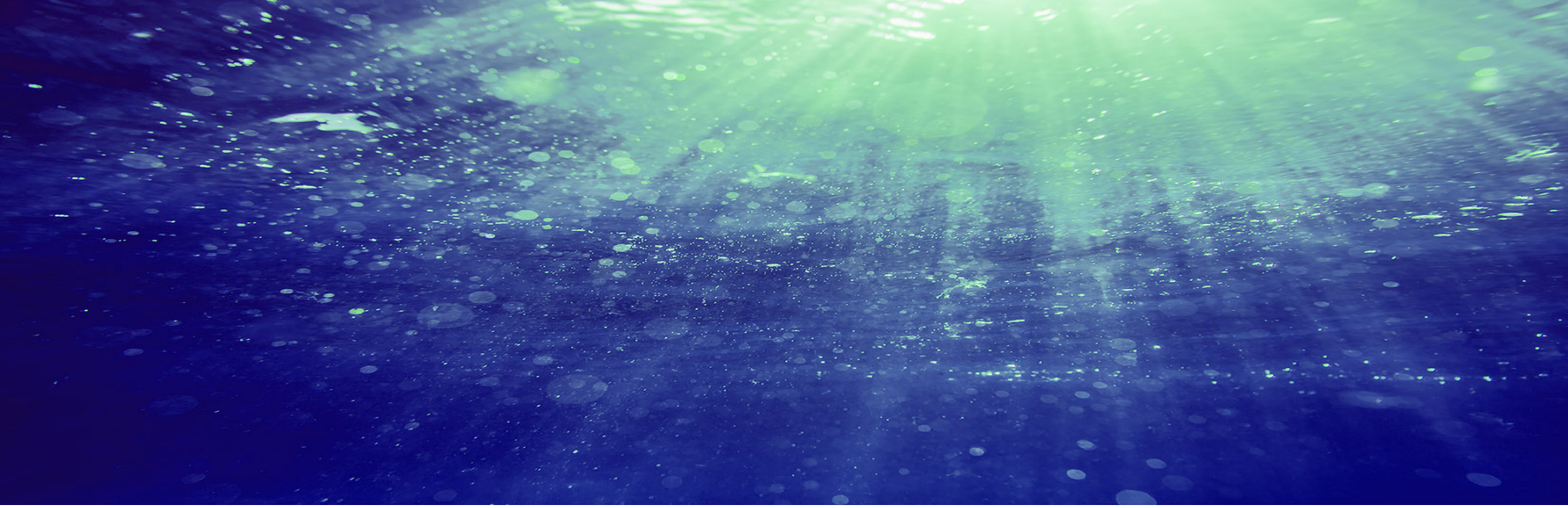


Certified Third-Party Auditing Organizations (C3PAOs): Approved organizations providing CMMC auditing services

Assessment Process | Attaining Certification

The CMMC-AB manages the interface between OSCs and the private, independent consulting and auditing organizations. While a C3PAO will conduct the audit, ultimate validation and certification will come from the CMMC-AB. Certification is not required to participate in bids, but it will be required upon contract award. OSCs will have the opportunity to dispute negative findings by the CMMC-AB.





Assessments

ankura

Assessment Process: Where to start?

Companies starting to consider their readiness to go through the CMMC certification process should consider starting with a baseline assessment. This assessment will ultimately enable the company to avoid creating duplicative structures and build on existing elements of its cybersecurity program.

Sample Elements of a CMMC Assessment:

- Preparation of a gap assessment
- Review of current policies and processes vs. CMMC framework
- Review of the efficacy of current controls vs. CMMC standard
- Development of evidence and artifact repository
- Preparation of implementable measures with timeline of actions and milestones
- Identify key organizational stakeholders (whole of org effort)

What not to do:

- Beware of “promise the moon”
- Focus on controls alone
- Wait to develop policies and procedures

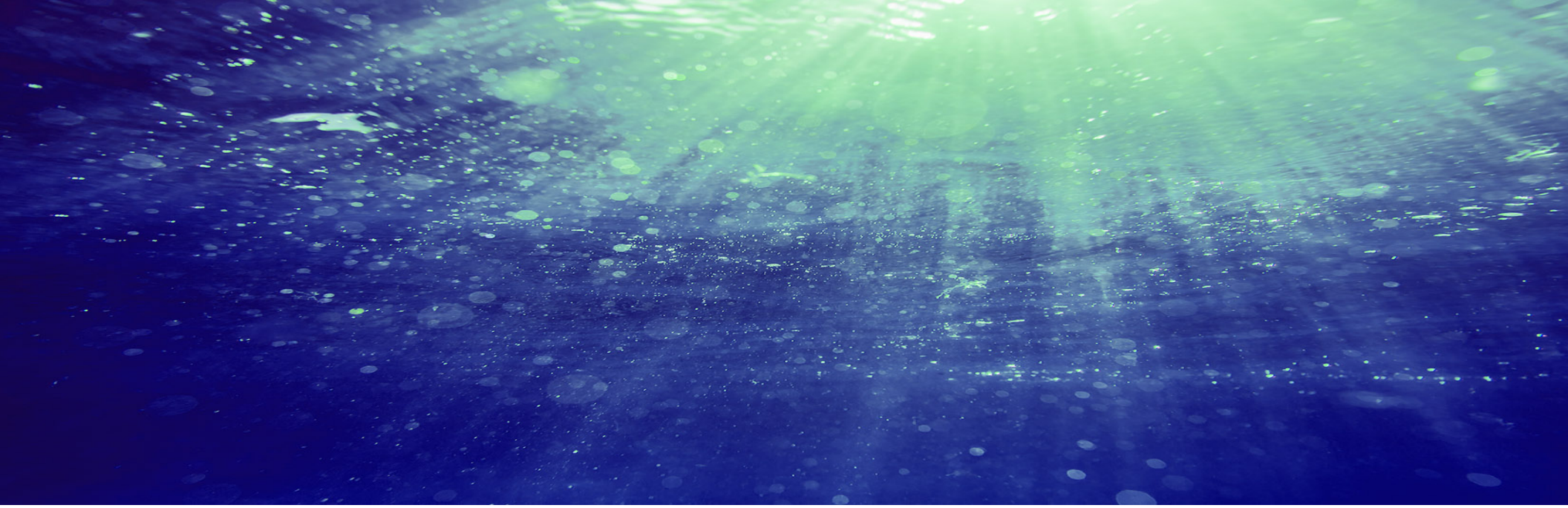
Assessment Process: Lessons Learned

Common areas of required enhancement:

- Lack of awareness of CUI environment (assessment scope)
- Failure to distinguish CUI in policies (CUI is expansive, it is not just ITAR)
- Documents are in not in order (draft form, does not match SSP, etc.)
- Lack of evidence to demonstrate practice implementation
- OT systems not effectively managed

Common obstacles to productive assessments:

- Wait to collect evidence
- Wait to engage stakeholders
- Wait to develop policies, processes, and procedures



CLOSING AND Q&A

ankura

Benefits of CMMC Compliance

The CMMC certification belongs to the organization which received it, and not the contract. It is valid for three years and can be used as a point of differentiation when responding to RFPs. The CMMC is a modern, comprehensive framework; and the practices mandated by the CMMC will improve the cybersecurity and IT efficiency of any organization.

1. Alignment to leading standards
2. Increased customer/partner trust
3. Reduction in incident response costs
4. Improved IT governance
5. Improved organizational resiliency

CMMC Seminar | September-October

Time	Topic
0830 - 0915	Introduction to the CMMC and threat landscape
0915 – 1100	CMMC requirements
1100 – 1200	Developing a CMMC compliance program
1200 – 1300	*Lunch & Roundtable Discussion*
1300 – 1400	CMMC audit process
1400 – 1500	Applying challenging controls
1500 – 1600	Managing supply chain relationships
1600 – 1700	Discussion and Q&A

Key Takeaways

- ✓ Understand the CMMC from high level to technical level
- ✓ Understand the assessment and certification process
- ✓ Understand the multiple paths to compliance
- ✓ Learn how to manage relationships with Primes
- ✓ Understand the business case for compliance
- ✓ Learn how to articulate CMMC compliance to business leaders

Q&A

If you have any additional questions or comments regarding Ankura or this presentation, or would like to schedule an organization-specific seminar, please send an email to Joseph M. Moyer at joseph.moyer@ankura.com or call at 571-212-2469.