AGC THE CONSTRUCTION ASSOCIATION

bakertilly now, for tomorrow.

Baker Tilly / AGC of America

March 17, 2021

A Practical Examination of CMMC for Construction

Jordan Howard
Director, Federal and Heavy Construction
The Associated General Contractors of America

Matt Gilbert
Principal, Risk Advisory
Baker Tilly

CMMC Overview

CMMC Overview

- Cybersecurity Maturity Model Certification (CMMC) is a cybersecurity model created by combining various cybersecurity standards and best practices
- The model's creation was funded and supported by the DoD
- CMMC builds upon existing regulations (e.g., FAR 52.204-21& DFARS 252.204-7012) where compliance is based on trust, by adding a verification component
- The purpose of the model is to support a process for certifying contractors
- Most organizations receiving funding from the DoD will need to be certified to qualify for future DoD acquisitions, with only exception potentially for commercial items
- The Model includes:
    - 17 capability domains
    - 43 capabilities
    - 5 processes across five levels to measure process maturity
    - 171 practices across five levels to measure technical capability

CMMC Practices

AGC THE CONSTRUCTION ASSOCIATION

bakertilly now, for tomorrow.

Level 1

Basic cyber hygiene

17 Practices

- Equivalent to all practices in FAR 48 CFR 52.204-21

Level 2

Intermediate cyber hygiene

72 Practices

- Comply with FAR
- Include a select subset of 48 practices from NIST SP800-171 r1
- Include additional 7 practices to support intermediate cyber hygiene

Level 3

Good cyber hygiene

130 Practices

- Comply with FAR
- Includes all practices from NIST SP800-171 r1
- Include additional 20 practices to support intermediate cyber hygiene

Level 4

Proactive

156 Practices

- Comply with FAR
- Includes all practices from NIST SP800-171 r1
- Includes a subset of 11 practices from Draft NIST SP 800-171B
- Include additional 15 demonstrate a proactive cybersecurity program

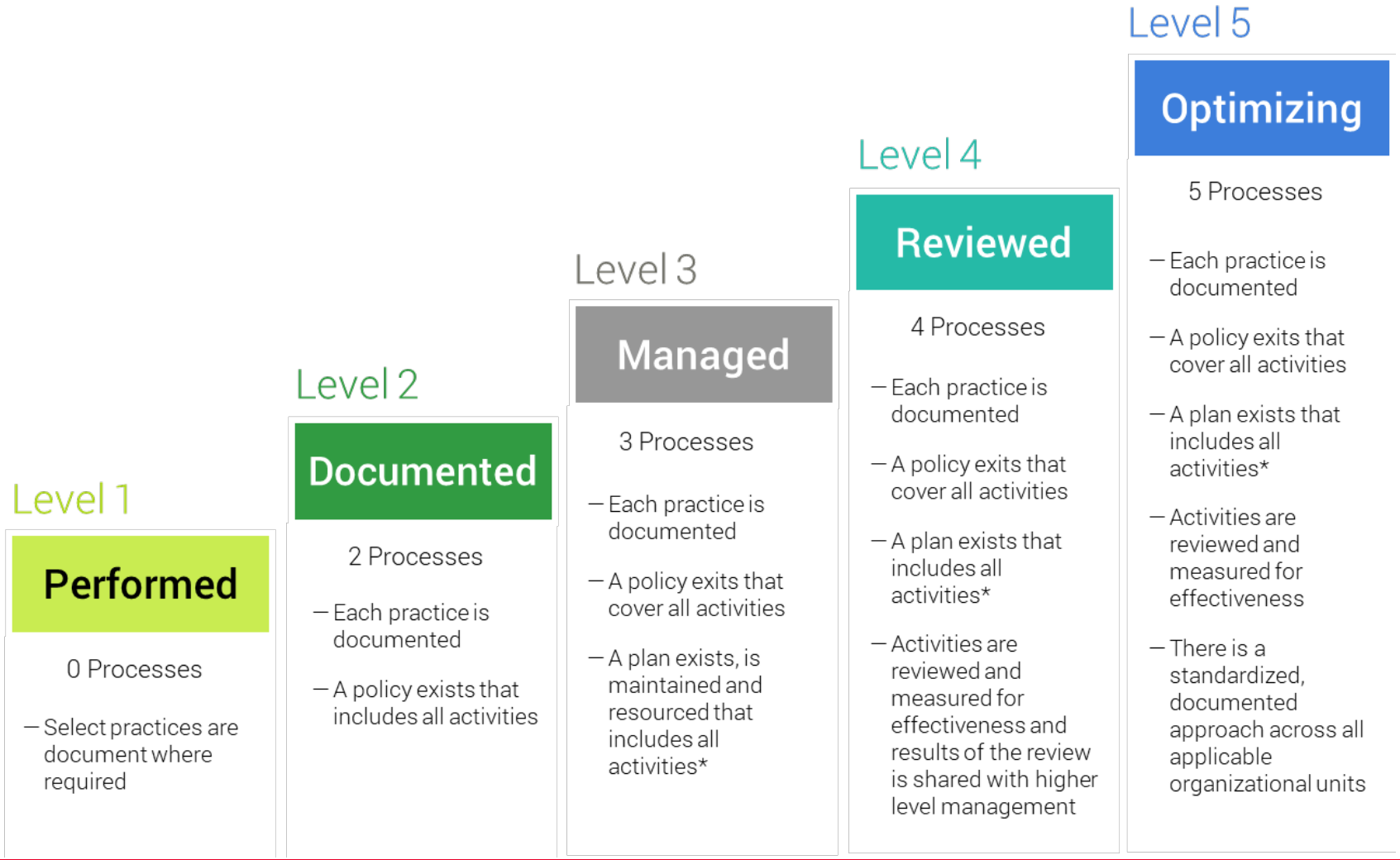
Level 5

Advanced/ progressive

171 Practices

- Comply with FAR
- Includes all practices from NIST SP800-171 r1
- Includes a subset of 4 practices from Draft NIST SP 800-171B
- Include additional 11 practices to support demonstrate an advances cybersecurity program

CMMC Processes



CMMC Domains

CMMC Domains

Role	Responsibilities
Assessors	Individuals who have successfully completed the background, training, and examination requirements as outlined by the CMMC AB and to whom a license has been issued. Assessors are not employed by the CMMC AB and may or may not be employed by the C3PAO
C3PAO	An entity with which at least two Assessors are associated and to which a license has been issued to engage with OSCs to complete their associated CMMC assessment.
CMMC AB	The accreditation body that establishes and oversees a qualified, trained, and high-fidelity community of assessors that can deliver consistent and informative assessments to participating organizations against a defined set of controls/best practices within the CMMC program
Organization Seeking Certification (OSC)	The organization that is going through the CMMC assessment process to receive a level of certification for a given environment(s)

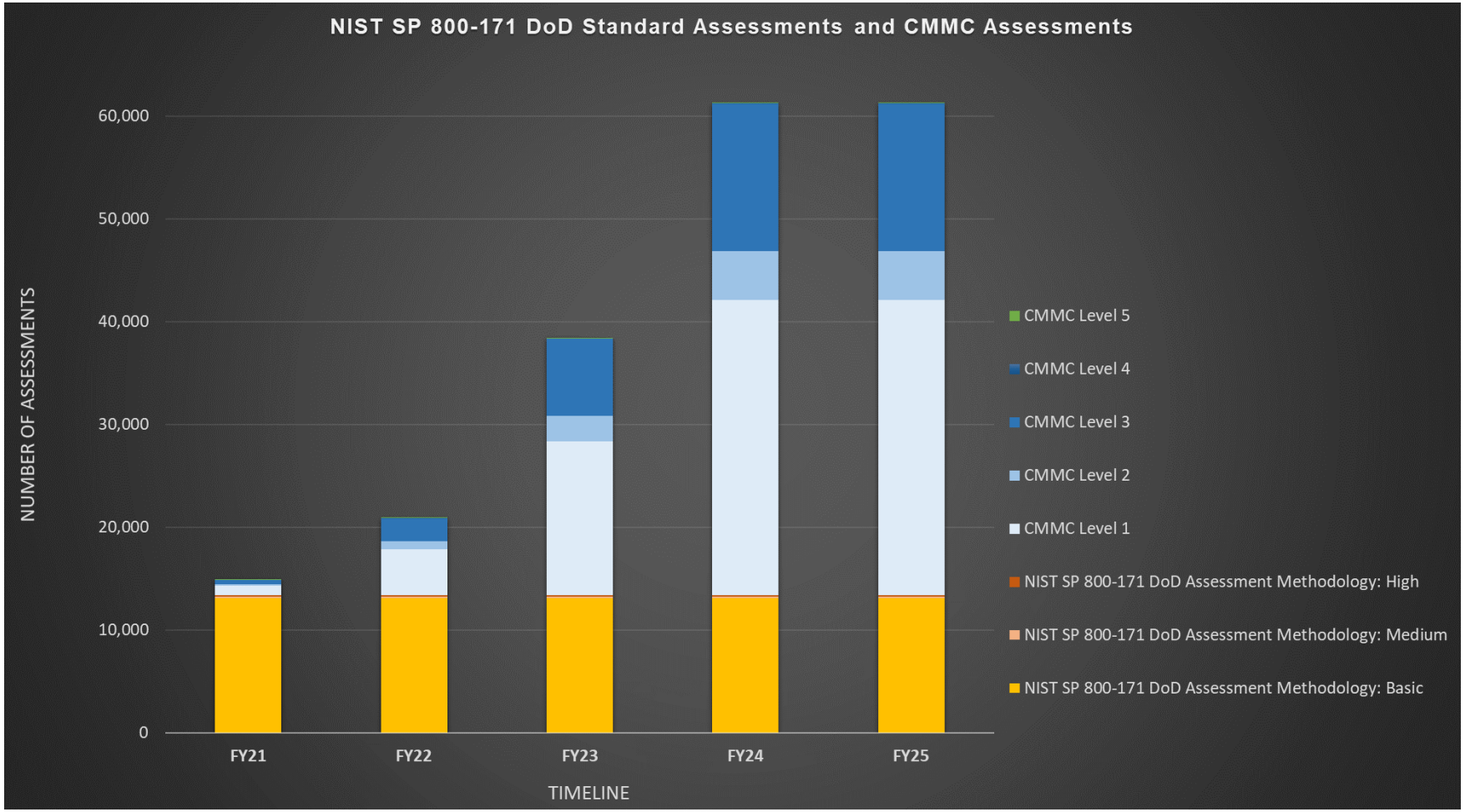
CMMC Phased Approach to RFP Release

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

From DoD Presentation dated Nov. 5, 2020

CMMC Phased Approach to Assessments



From DoD Presentation dated Nov. 5, 2020

DFARS Clauses

Related FAR and DFARS Clauses

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

- *New Interim Rule:* DFARS clause 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7020, (NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

FCI and CUI defined

FCI (Federal Contract Information) - Federal contract information means 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 (such as on public Web sites) or simple transactional information, such as necessary to process payments. Source: 48 CFR § 52.204-21

CUI (Controlled Unclassified Information) - Information that requires safeguarding or dissemination controls pursuant to and consistent with the law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. Source: E.O. 13556 (adapted)

DFARS 252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting

- Covers ***information***, not just the ***information system*** itself
- Incorporates NIST SP 800-171
- Requires implementation of 110 security requirements on ""covered contractor information systems
- Document in System Security Plan & Plans of Action & Milestones (POAMs) those requirements not yet implemented and when they will be implemented
- Must "***rapidly report***" cyber incident within "***72 hours of discovery***"
    - Report "whatever information is available"
    - Continuing obligation to disclose new information
    - Must preserve and protect images of all known affected information systems for at least 90 days to allow DOD to request the media
- A cyber incident is defined as: "actions taken through the use of computer networks that result in a compromise or an actual or potential adverse effect on an information system and/or the information residing therein"
- Much faster than the mandatory disclosures required under FAR 52.203-13 (Contractor Code of Business Ethics)

DFARS 252.204-7019 & 7020 NIST SP 800-171 DoD Assessment Requirements

- *New DoD assessment methodology!*
- Requires contractors subject to DFARS 252.204-7012 to self complete a Basic Assessment and upload the resulting score into the Supplier Risk Management System (SPRS) prior to contract award
- Medium and High Assessments may be required and will be completed by the government (DIBCAC)
- Requires contractors to flow same requirement down to subcontractors in "all subcontracts and other contractual instruments"
- 7020 Clause for SP 800-171 Assessments
    - "information systems relevant to its offer"
- Transition clause until October 1, 2025

CMMC Assessment – what to expect?

Audit or Assessment

Audit

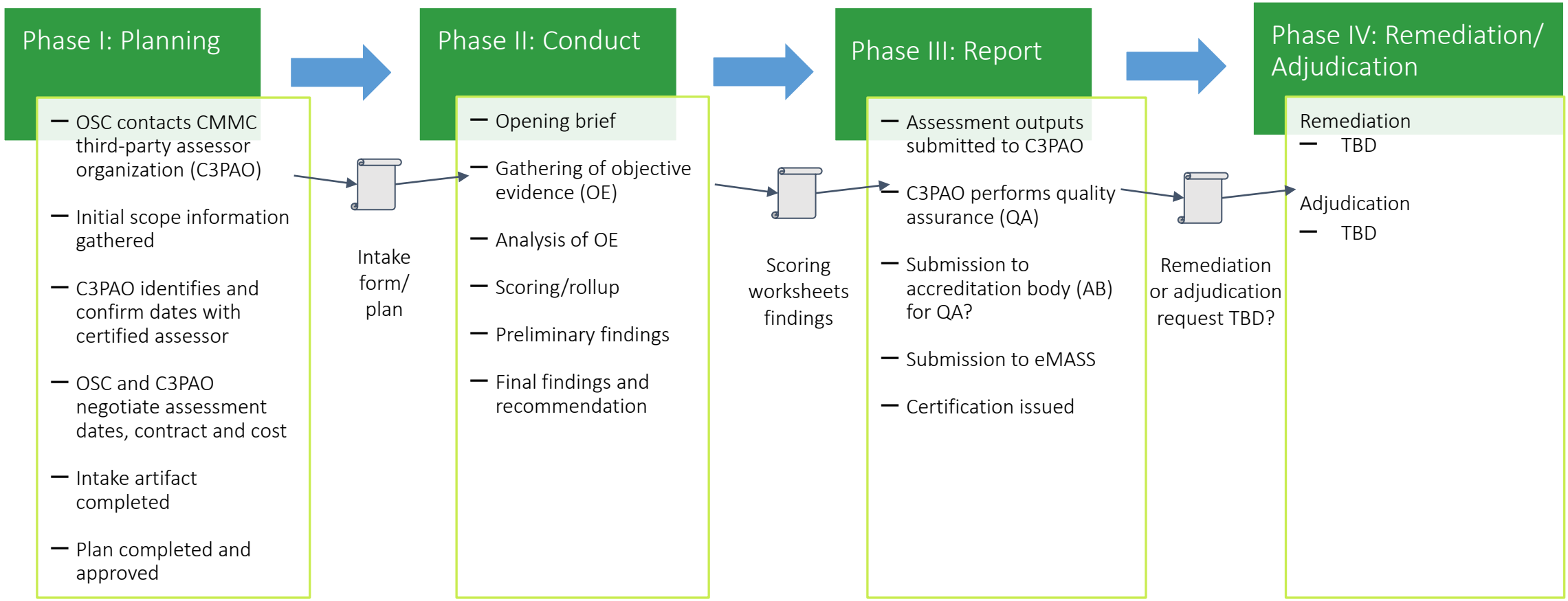
An official inspection of an individual's or organization's accounts, typically by an independent body.

Assessment

The evaluation or estimation of the nature, quality or ability of someone or something.

To achieve the objective of levels 2+ you have to be conducting an assessment.

Notional Assessment Process



Assessment Participants

- OSC assessment sponsor
- OSC point of contact
- C3PAO
- Lead assessor
- Assessment team
- OSC representatives (practice/process owners)
- CMMC-AB

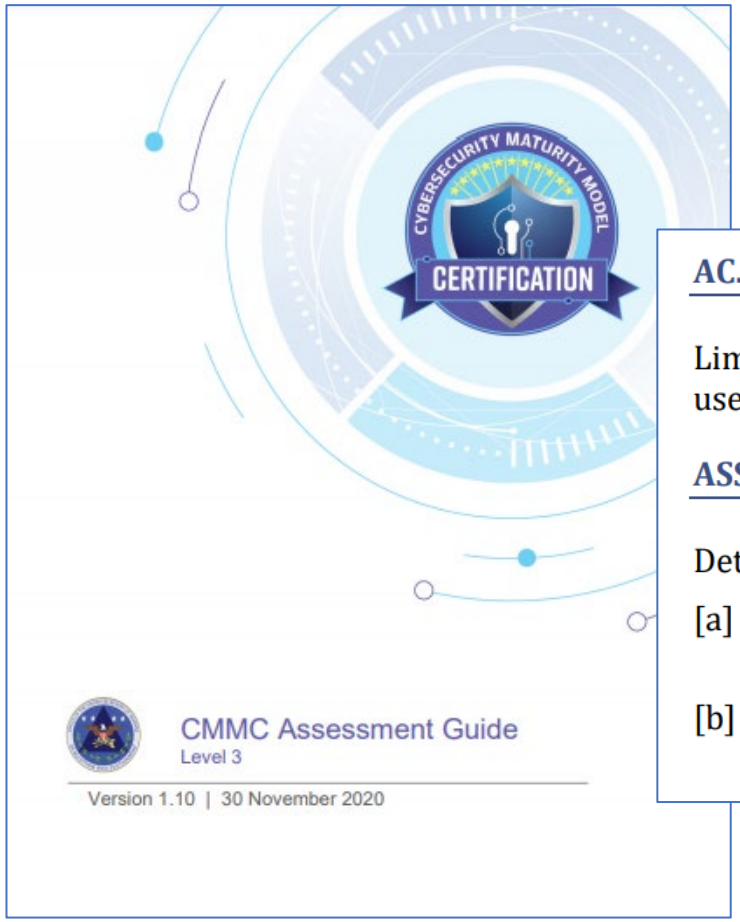
Notional Intake Requirements

- Basic information about the OSC and the C3PAO

- The OSC should be prepared to provide information such as:
    - Target level
    - Scope and Locations
    - Practices to be inherited (i.e. reciprocity)
    - Practices that are N/A
    - Confirmations related to CUI
    - CAGE codes that scope applies to similar to SPRS

- Agreement between the OSC and C3PAO related to timing and assessment team.

Assessment Guides



The Assessment Guides define the objectives that the assessor will evaluate. Here is an example for AC.1.002:

AC.1.002

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

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

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.

https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf

Methods for Gathering and Analyzing Objective Evidence

- **Examine** – The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.

- **Interview** – The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.

- **Test** – The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time.

Questions?

Contact Information

Matt Gilbert
Principal – CMMC Leader,
Risk Advisory Practice
CMMC Certified Provisional Assessor, CISA, CRISC
matt.gilbert@bakertilly.com

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2020 Baker Tilly US, LLP.