RESTON

I’ve Got a Gap in my CAP

Panel

2025

www.cs2.cloud/reston

Our Panel

Matt Bruggeman, Dir of GTM Federal

A-Lign (C3PAO)

Favorite Highschool Memory:

Best Movie of All Time:

Number of CMMC L2 Assessments to Date:

Our Panel

Fernando Machado, Managing Principal,

CISO | Lead CCA

Cybersec Investments (C3PAO)

Favorite Highschool Memory:

Best Movie of All Time:

Number of CMMC L2 Assessments to Date:

Our Panel

Logan Therrien, Chief Strategy Officer

Lead CCA

Kieri (C3PAO)

Favorite Highschool Memory:

Best Movie of All Time:

Number of CMMC L2 Assessments to Date:

Our Moderator

Joy Beland, VP Cybersecurity Compliance

Lead CCA & PI

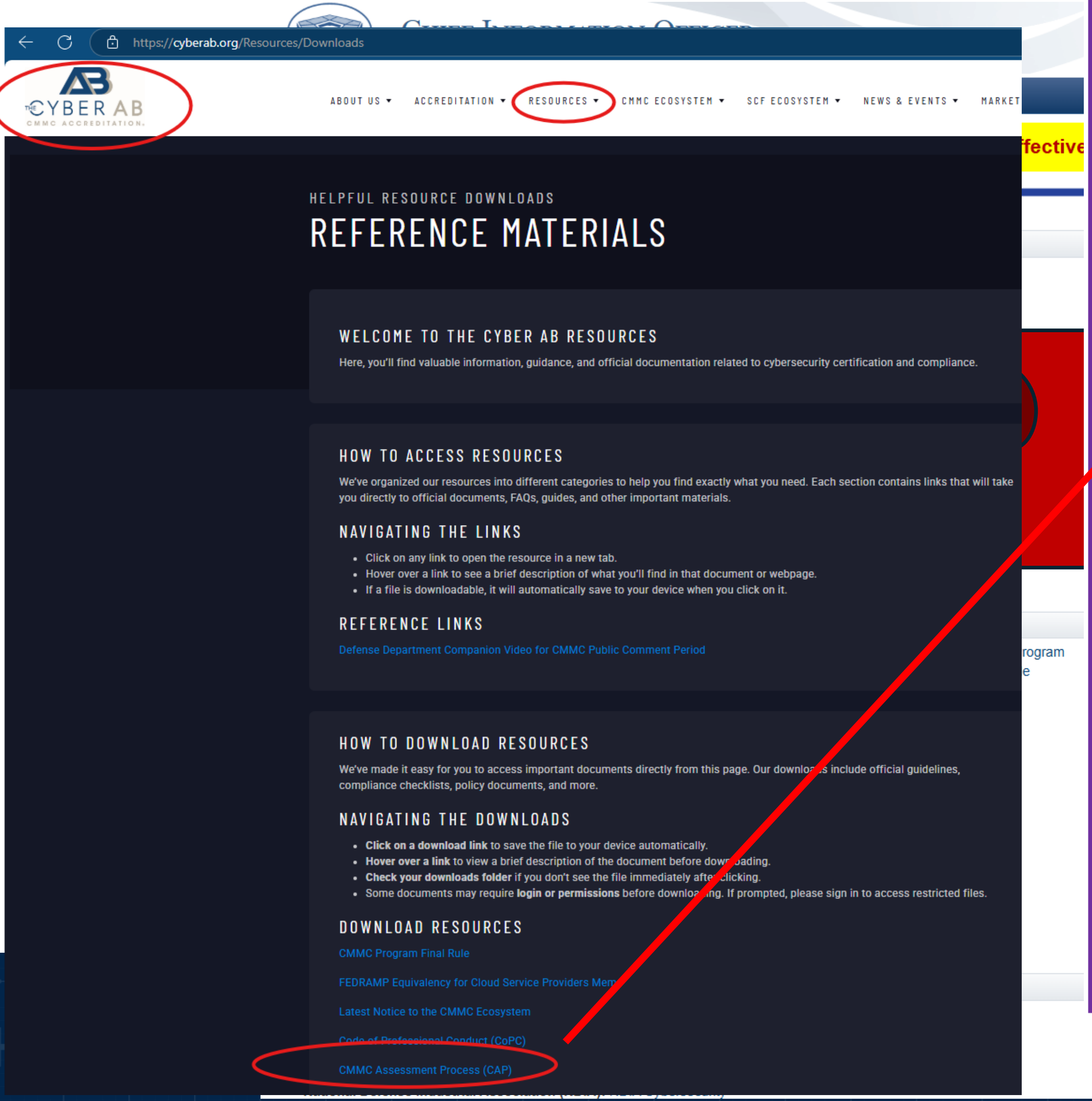
Summit 7 (RPO, ESP)

Favorite Highschool Memory:

Best Movie of All Time:

Number of CMMC L2 Assessments to Date:

Where Do I Get The “CAP”



HELPFUL RESOURCE DOWNLOADS

REFERENCE MATERIALS

WELCOME TO THE CYBER AB RESOURCES

Here, you'll find valuable information, guidance, and official documentation related to cybersecurity certification and compliance.

HOW TO ACCESS RESOURCES

We've organized our resources into different categories to help you find exactly what you need. Each section contains links that will take you directly to official documents, FAQs, guides, and other important materials.

NAVIGATING THE LINKS

- Click on any link to open the resource in a new tab.
- Hover over a link to see a brief description of what you'll find in that document or webpage.
- If a file is downloadable, it will automatically save to your device when you click on it.

REFERENCE LINKS

Defense Department Companion Video for CMMC Public Comment Period

HOW TO DOWNLOAD RESOURCES

We've made it easy for you to access important documents directly from this page. Our downloads include official guidelines, compliance checklists, policy documents, and more.

NAVIGATING THE DOWNLOADS

- **Click on a download link** to save the file to your device automatically.
- **Hover over a link** to view a brief description of the document before downloading.
- **Check your downloads folder** if you don't see the file immediately after clicking.
- Some documents may require **login or permissions** before downloading. If prompted, please sign in to access restricted files.

DOWNLOAD RESOURCES

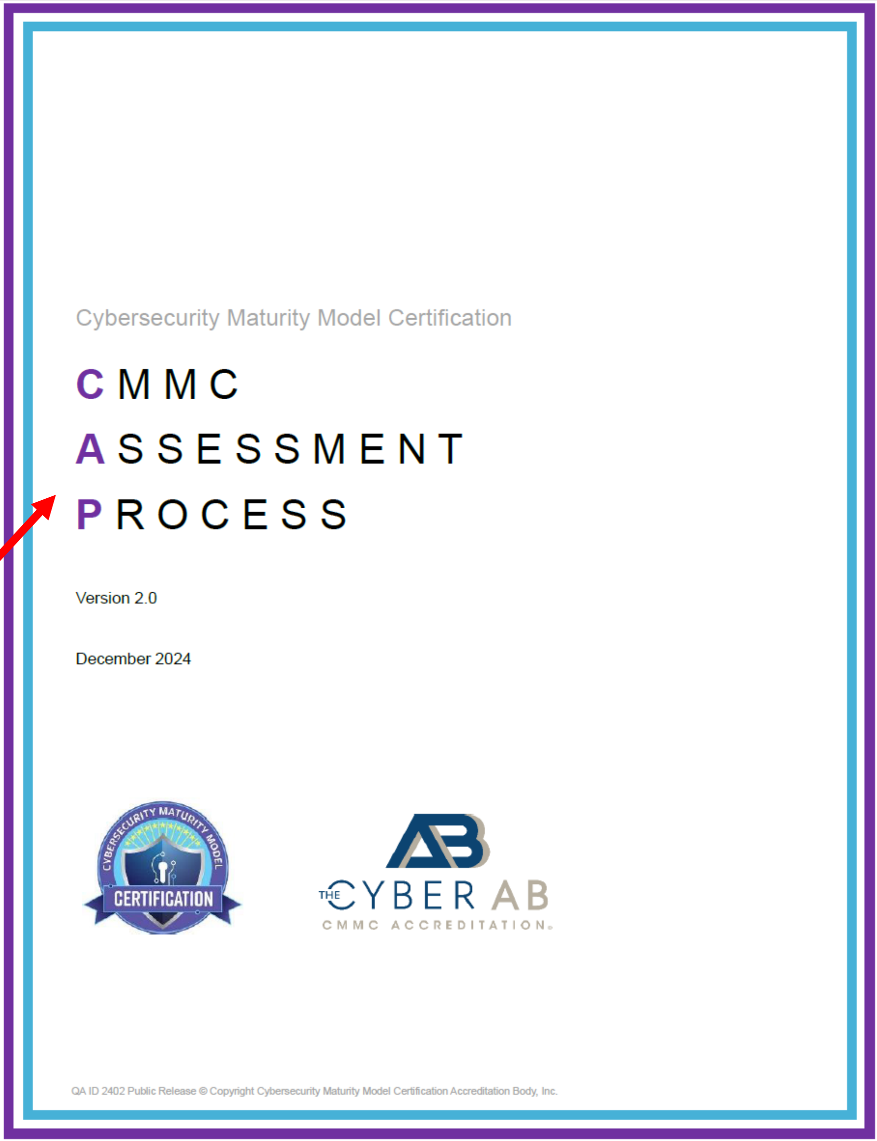
CMMC Program Final Rule

FEDRAMP Equivalency for Cloud Service Providers Mem

Latest Notice to the CMMC Ecosystem

Code of Professional Conduct (CoPC)

CMMC Assessment Process (CAP)



Cybersecurity Maturity Model Certification

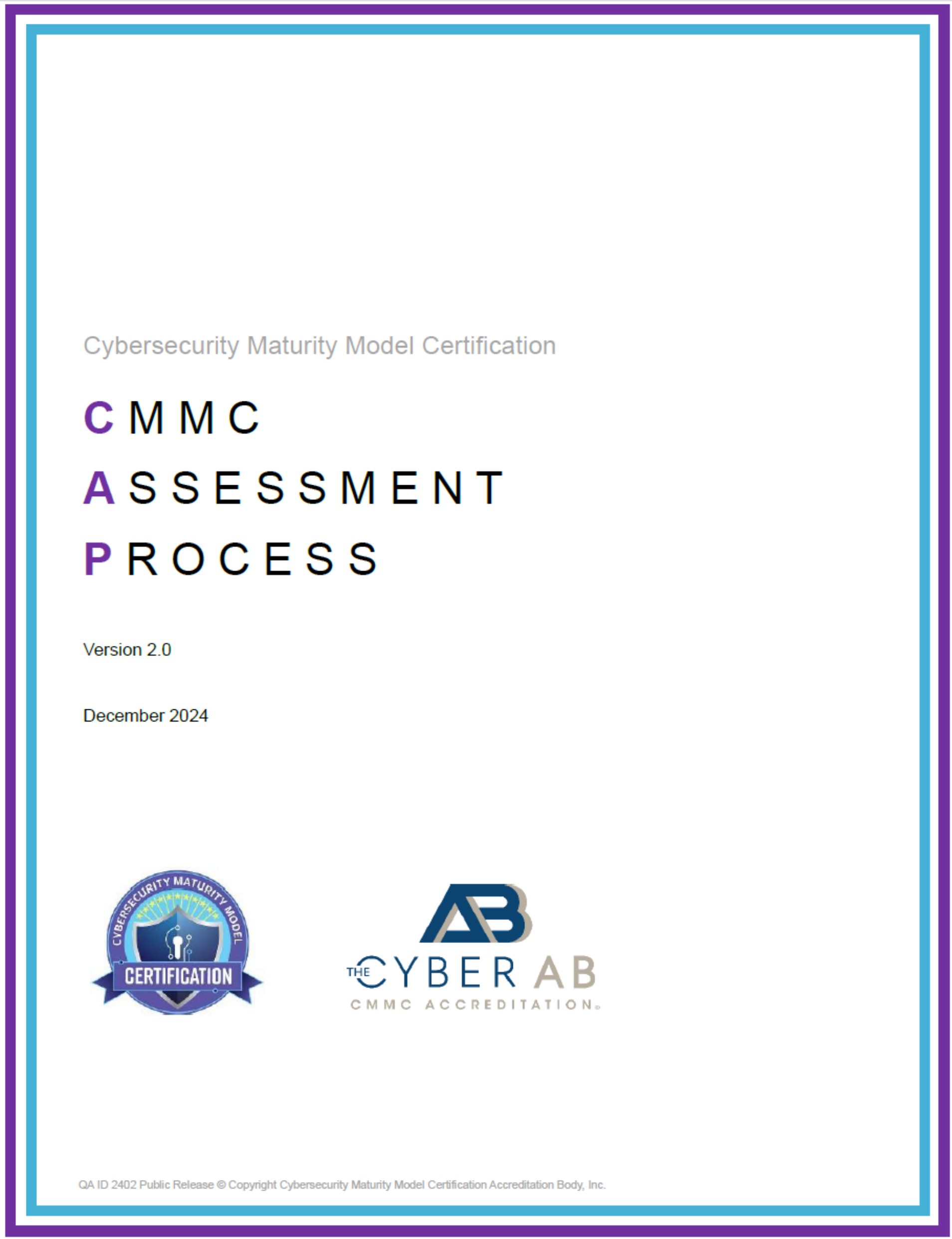
CMMC ASSESSMENT PROCESS

Version 2.0

December 2024

QA ID 2402 Public Release © Copyright Cybersecurity Maturity Model Certification Accreditation Body, Inc.

What is the "CAP"



Cybersecurity Maturity Model Certification

CMMC ASSESSMENT PROCESS

Version 2.0

December 2024

Roles and Responsibilities

Preliminary Proceedings

Phase 1: CONDUCT THE PRE-ASSESSMENT

Phase 2: ASSESS CONFORMITY TO SECURITY REQUIREMENTS

Phase 3: COMPLETE AND REPORT ASSESSMENT RESULTS

Phase 4: ISSUE CERTIFICATE AND CLOSE OUT POA&M

Level Set

Roles and Responsibilities

Preliminary Proceedings

Phase 1: CONDUCT THE PRE-ASSESSMENT

Phase 2: ASSESS CONFORMITY TO SECURITY REQUIREMENTS

Phase 3: COMPLETE AND REPORT ASSESSMENT RESULTS

Phase 4: ISSUE CERTIFICATE AND CLOSE OUT POA&M

What are some surprises you want the OSC to know about?

Level Set

Roles and Responsibilities

Preliminary Proceedings

Phase 1: CONDUCT THE PRE-ASSESSMENT

Phase 2: ASSESS CONFORMITY TO SECURITY REQUIREMENTS

Phase 3: COMPLETE AND REPORT ASSESSMENT RESULTS

Phase 4: ISSUE CERTIFICATE AND CLOSE OUT POA&M

Definition of an **External** Service Provider:

- Cloud Service Provider
- MSP/MSSP
- *HQ Providing Data Access or Information System Support to subsidiary or satellite locations*

"An ESP would be considered a CSP when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction on the part of the OSA."

Gap #1

Per 32 CFR Part 170 “CMMC Final Rule”

If an OSA utilizes an ESP, including a Cloud Service Provider (CSP), that does not process, store, or transmit CUI, the ESP does not require its own CMMC assessment. There is nothing in the rule that precludes an ESP, that is not a CSP, from voluntarily requesting a C3PAO assessment. A C3PAO may perform such an assessment if the ESP makes that business decision.

An ESP that is seeking CMMC assessment will need to obtain a CAGE code and an account in SPRS to enable the reporting of its assessment results via CMMC eMASS. A SPRS account is required to complete the CMMC annual affirmation requirement included in DoD contracts that include a CMMC certification requirement.

ESPs that are not CSPs may request voluntary CMMC assessments of their environment and use that as a business discriminator. The marketplace for ESP services will adjust to find the efficient manner for ESPs to support OSA assessments that may include their services.

Assessing ESPs - Should it be the same as an OSC? Why and why not?

Gap #2

Per CAP 2.0

In the event the OSC is utilizing a "non-CSP" ESP that voluntarily attained a Level 2 or Level 3 Certificate of CMMC Status, the Assessment Team should anticipate and accept a ***lower level of effort*** *on behalf of the ESP during the OSC's assessment. Specifically, if the Assessment Team confirms the ESP is in possession of a valid Certificate of CMMC Status, it may consider those security requirements under the responsibility of the ESP to be in a validated state. The Assessment Team shall still ensure that each* ***inherited*** *security requirement from the ESP is still implemented and currently being maintained in the state under which it was originally assessed and/or have the ESP attest to same. ESP personnel still need to participate during Phase 2 of the OSC's assessment to answer questions of the Assessment Team.*

- What does "Lower level of effort" actually look like?
- What does Inheritance look like? Non-Duplication?

Gap #3

Per 32 CFR Part 170 “CMMC Final Rule”

The use of an ESP, its relationship to the OSA, and the services provided need to be documented in the OSA’s System Security Plan and described in the ESP’s service description and customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided.

Per CAP 2.0

The Assessment Team shall evaluate that the Customer Responsibility Matrix (CRM) of an ESP is up-to date, includes all relevant parties with security responsibilities, and addresses all in-scope CMMC security requirements performed wholly, partially, or jointly by the ESP.

- What ESP Documentation are you expecting the OSC to provide? What about their CSP’s who are FedRAMP Moderate or High?

Gap #4

Per CAP 2.0

Assessors may re-evaluate NOT MET security requirements during the assessment and for ten (10) business days following the active assessment period (i.e., the conclusion of Phase 2 activities) ***in accordance with the requirements established in 32 CFR §170.17(c)(2).***

How this applies to 1,3,5 pointers? Real life experience with this?
What type of Not Met control implementation would be considered unacceptable for the OSA to fix the 10-day window following the active assessment period, if any?

Gap #5

Per CAP 2.0

Another consideration of framing the assessment involves determining assessment location(s), including what security requirement objectives of the assessment might be assessed virtually or in-person on the OSC premises. The Lead CCA and/or the C3PAO should consider the optimal logistical approach for implementation validation of the following 18 CMMC security requirement objectives to ensure adequate assessment scope and depth: (goes on to list mostly physical security controls)

Are there any caveats or challenges you're seeing in the scoping call, to help determine if an onsite visit is needed?

Closing Thoughts?

Questions?

Joy.beland@summit7.us 310-590-9288 https://www.linkedin.com/in/joy-belinda-beland/