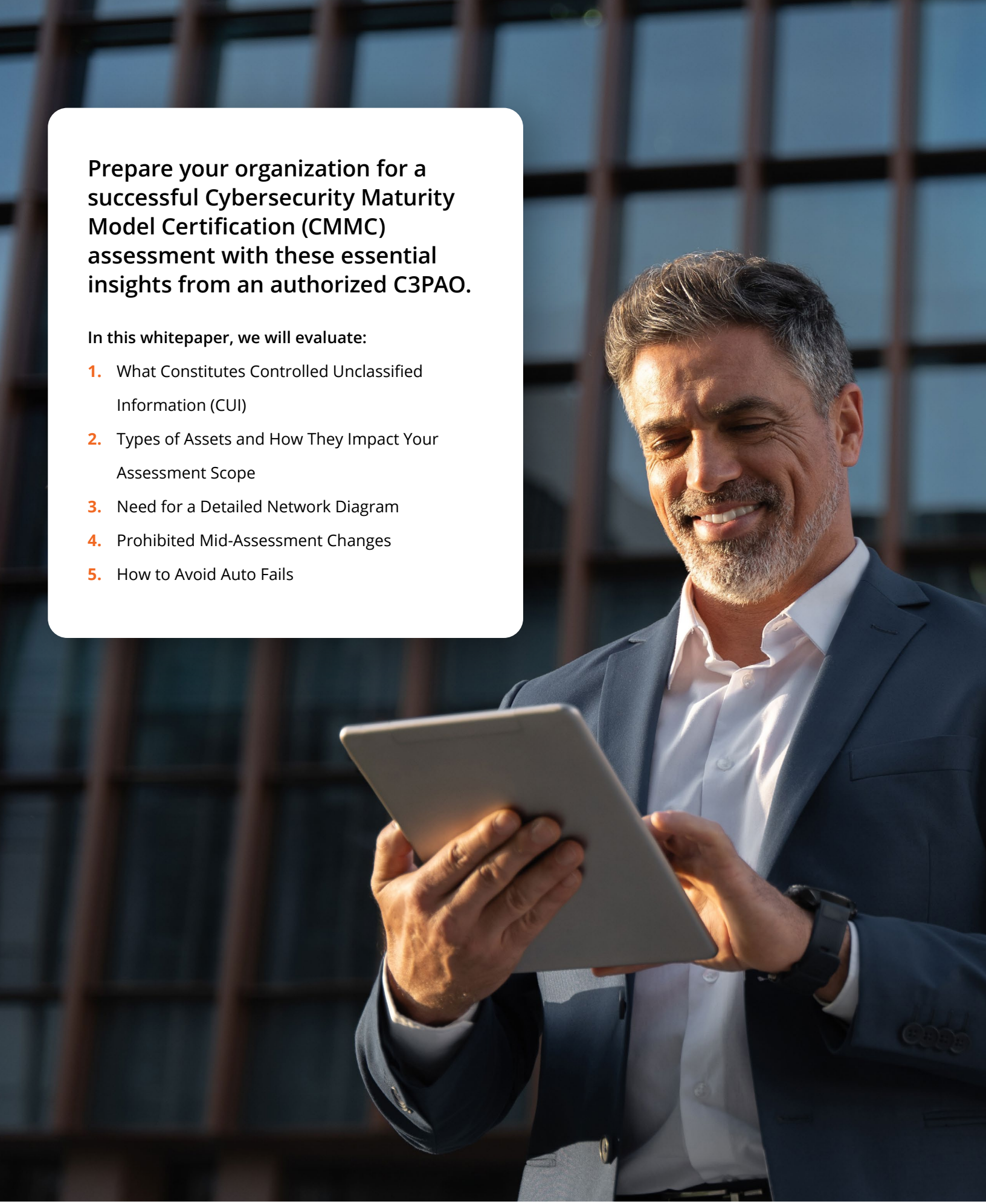
S|3 SPECIALIZED SECURITY SERVICES

5 THINGS YOU SHOULD KNOW ABOUT CMMC ASSESSMENTS



Prepare your organization for a successful Cybersecurity Maturity Model Certification (CMMC) assessment with these essential insights from an authorized C3PAO.

In this whitepaper, we will evaluate:

1. What Constitutes Controlled Unclassified Information (CUI)
2. Types of Assets and How They Impact Your Assessment Scope
3. Need for a Detailed Network Diagram
4. Prohibited Mid-Assessment Changes
5. How to Avoid Auto Fails

1. What Constitutes Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) includes sensitive data that is not classified but still requires safeguarding. If your organization processes, stores, or transmits CUI, you must implement and demonstrate compliance with applicable CMMC practices. Knowing which assets interact with CUI is foundational to correctly scoping your assessment.

2. Types of Assets and How They Impact Your Assessment Scope

Not all assets are treated equally under CMMC, so proper classification is critical.

- **Security Protection Assets**

  These provide security functionality such as firewalls, VPNs, and monitoring tools – even if they don't process CUI directly. These are in-scope and assessed against applicable CMMC practices.

- **Contractor Risk Managed Assets**

  These do not handle CUI but may still be part of your environment. If they are clearly separated and documented, they may be assessed differently.

- **Specialized Assets**

  This includes OT, IoT, and test equipment. These are documented in the System Security Plan (SSP) but typically not assessed against CMMC practices.

- **Out-of-Scope Assets**

  Assets that cannot process, store, or transmit CUI and are logically or physically separated from in-scope systems. They are not part of the CMMC assessment.

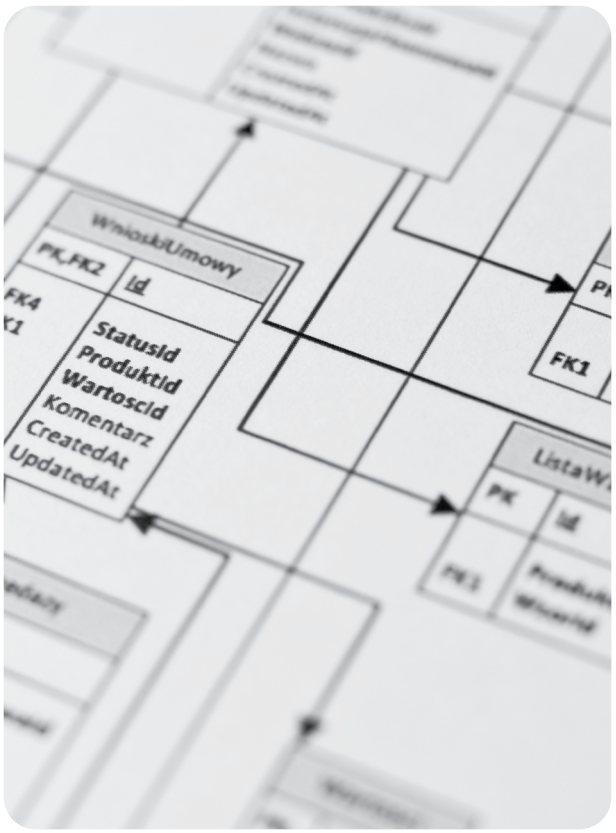
The clearer your asset inventory and classification, the smoother your assessment process will be.

3. A Detailed Network Diagram is Non-Negotiable

A well-prepared network diagram can significantly reduce confusion and delays during your assessment.

Your network diagram must clearly illustrate in-scope systems, boundary protections, segmentation, and security services. It helps the assessor understand your architecture and ensures the appropriate application of CMMC requirements.

The diagram should also show the relationships between CUI, security protection assets, managed assets, and any segmentation strategies in place.



4. You Can't Change Things Mid-Assessment

CMMC assessments are point-in-time evaluations. This means:

- Technical or configuration changes to remediate a "Not Met" requirement **won't** be re-scored during the assessment period.
- Limited documentation changes are allowed, but only up to five updates. These must be minor clarifications and **cannot** materially impact the assessment outcome (e.g., clarifying existing practices, not adding new controls).
- Any documentation change that requires deeper review or alters prior assessments findings will **not** be accepted and may result in a "Not Met" finding.

Needless to say, advance preparation is key to avoiding costly surprises during the formal assessment window.

5. You Can Avoid Auto Fails

Some CMMC requirements carry more weight than others. Missing these critical requirements leads to automatic disqualification, even if your overall score is strong. In other words, if you miss them, you cannot pass, even with a high overall score.

These auto fail requirements vary slightly between Level 1 and Level 2 assessments, but the impact is the same: Missing any of them will prevent certification.

Level 1 Auto Fails

For Level 1 self-assessments:

- All 17 practices must be met.
- POA&Ms (Plans of Action and Milestones) are not permitted under any circumstances.

Level 2 Auto Fails

Organizations may use a POA&M to achieve a Conditional Level 2 status, but only if:

- The overall score is 80% or higher
- None of the auto fail requirements are marked "Not Met."

The following requirements cannot be included on a Level 2 POA&M:

- **High-value controls worth 3 or 5 points** are automatically excluded.
    - Exception: SC.L2-3.13.11 (CUI Encryption) may be included if encryption is in place but not FIPS-validated.
- **Six 1-point requirements** also cannot be failed or placed on a POA&M:
    - **AC.L2-3.1.20** – External Connections (CUI)
    - **AC.L2-3.1.22** – Control Public Information (CUI)
    - **CA.L2-3.12.4** – System Security Plan
    - **PE.L2-3.10.3** – Escort Visitors (CUI)
    - **PE.L2-3.10.4** – Physical Access Logs (CUI)
    - **PE.L2-3.10.5** – Manage Physical Access (CUI)

If any of these requirements are marked "Not Met," your organization cannot receive a conditional pass for Level 2, even if your overall score meets the 80% threshold.

Ready for Your CMMC Assessment?

CMMC certification is quickly becoming essential for contractors that want to win and retain Department of Defense contracts. It demonstrates your commitment to protecting sensitive information and meeting evolving federal requirements, making it a clear signal of trust and operational readiness.

As both an authorized Third-Party Assessment Organization (C3PAO) and a Registered Provider Organization (RPO), S3 Security is uniquely positioned to support your organization through every stage of the CMMC process. With more than 25 years of cybersecurity experience, we help you:

- Accurately scope your environment
- Align documentation and controls to CMMC requirements
- Avoid common missteps that can lead to delays or disqualification

Whether you're just beginning your readiness journey or preparing for a formal assessment, our team delivers the expertise and support you need to move forward with confidence.

Do not wait for compliance deadlines to arrive. Contact S3 Security today to begin take the first steps on your path to CMMC certification and strengthen your position as a trusted DoD contractor.

Learn more by clicking here or visiting:

s3security.com/compliance-assessment-services/cmmc-assessments/