Cybersecurity Maturity Model Certification (CMMC)

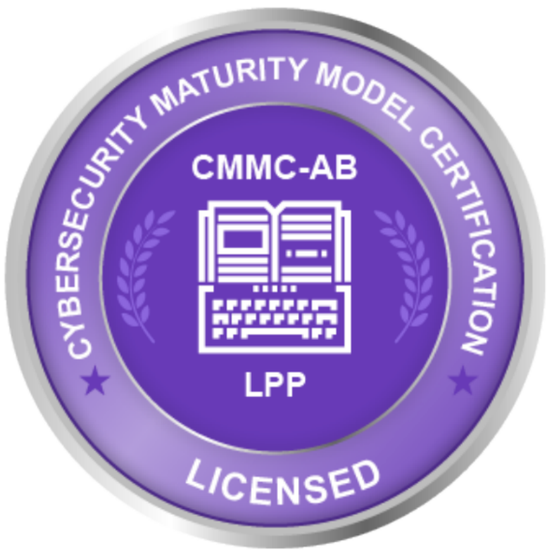
Everything you need to know about compliance, assessments, and getting certified

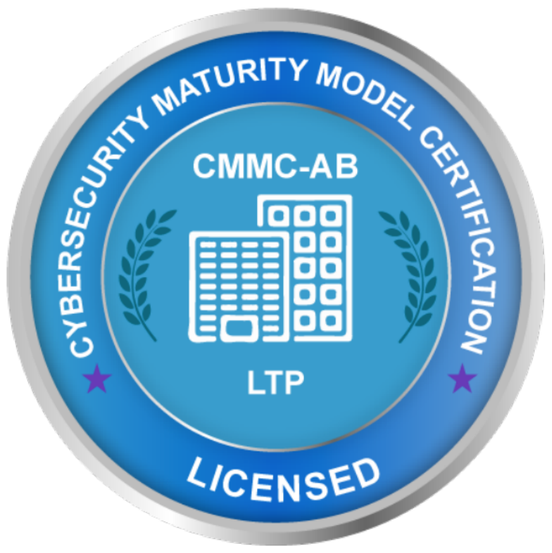
CSG Technologies

What is CMMC Famework?

The Department of Defense (DoD) supply chain and the Defense Industrial Base (DIB) it supports are continuously under threat by malicious actors. The theft of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) doesn't just stifle innovation and undercut U.S. technical advantages, it significantly increases the risk to national security.

To reduce this risk, the DoD released the CMMC framework, which is intended to assess and enhance the cybersecurity posture of the more than 300,000 companies that contribute towards the research, engineering, development, acquisition, production, delivery, sustainment and operation of DoD systems, networks, installations, capabilities and services.





CSG Technologies

Inside the CMMC requirements

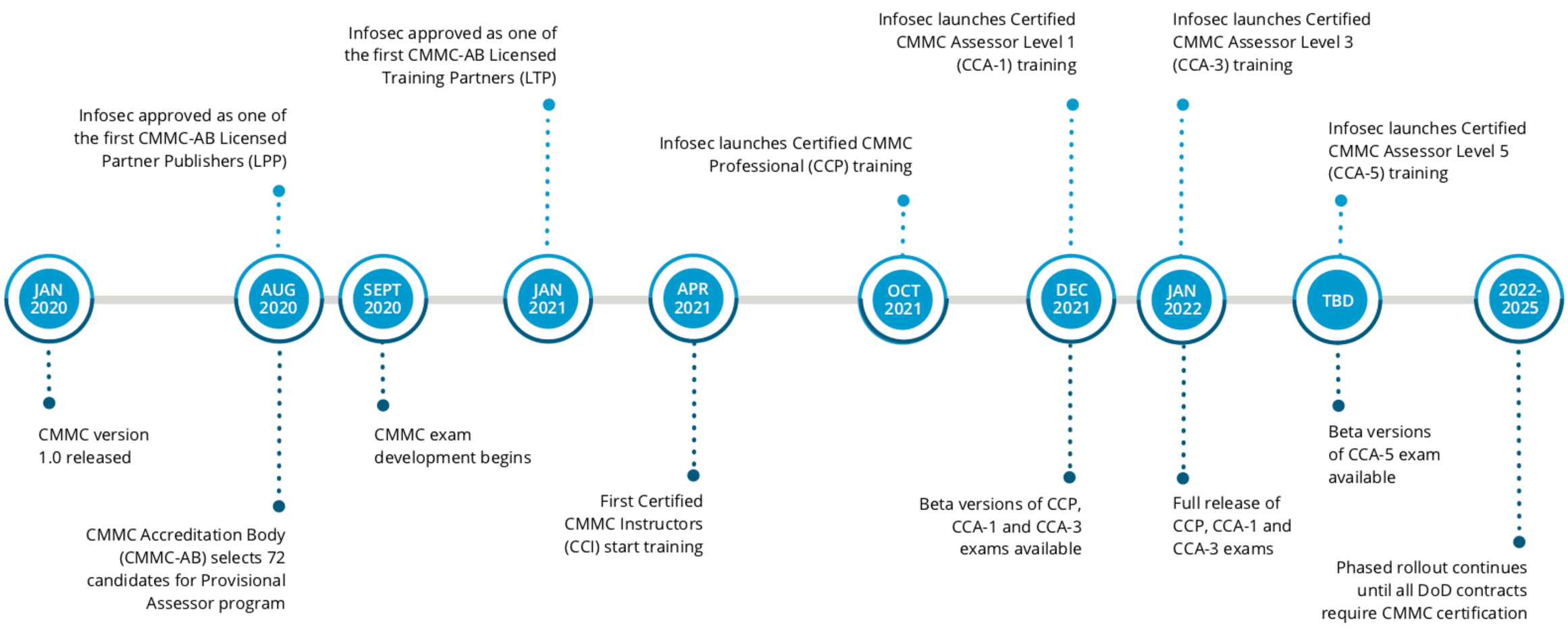
Although the CMMC framework is new, many of the security requirements within it are not. Of the 171 practices included in CMMC, 110 of them are specified in NIST SP 800-171 Rev. 2. Additional practices and processes are drawn from other standards, references and sources, such as:

- NIST SP 800-53
- Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 "Critical Security Controls for Effective Capability in Cyber Defense"
- Computer Emergency Response Team (CERT) Resilience Management Model (RMM) v1.2

CMMC builds upon existing regulation (DFARS 252.204-7012) by adding a certification program to verify the implementation of processes and practices across five cybersecurity maturity levels.

CMMC Timeline

When will you be affected?



Understanding the 5 CMMC Maturity Levels

The CMMC framework contains five maturity levels, with Level 5 being the highest. The processes and practices required for each level are aligned around:

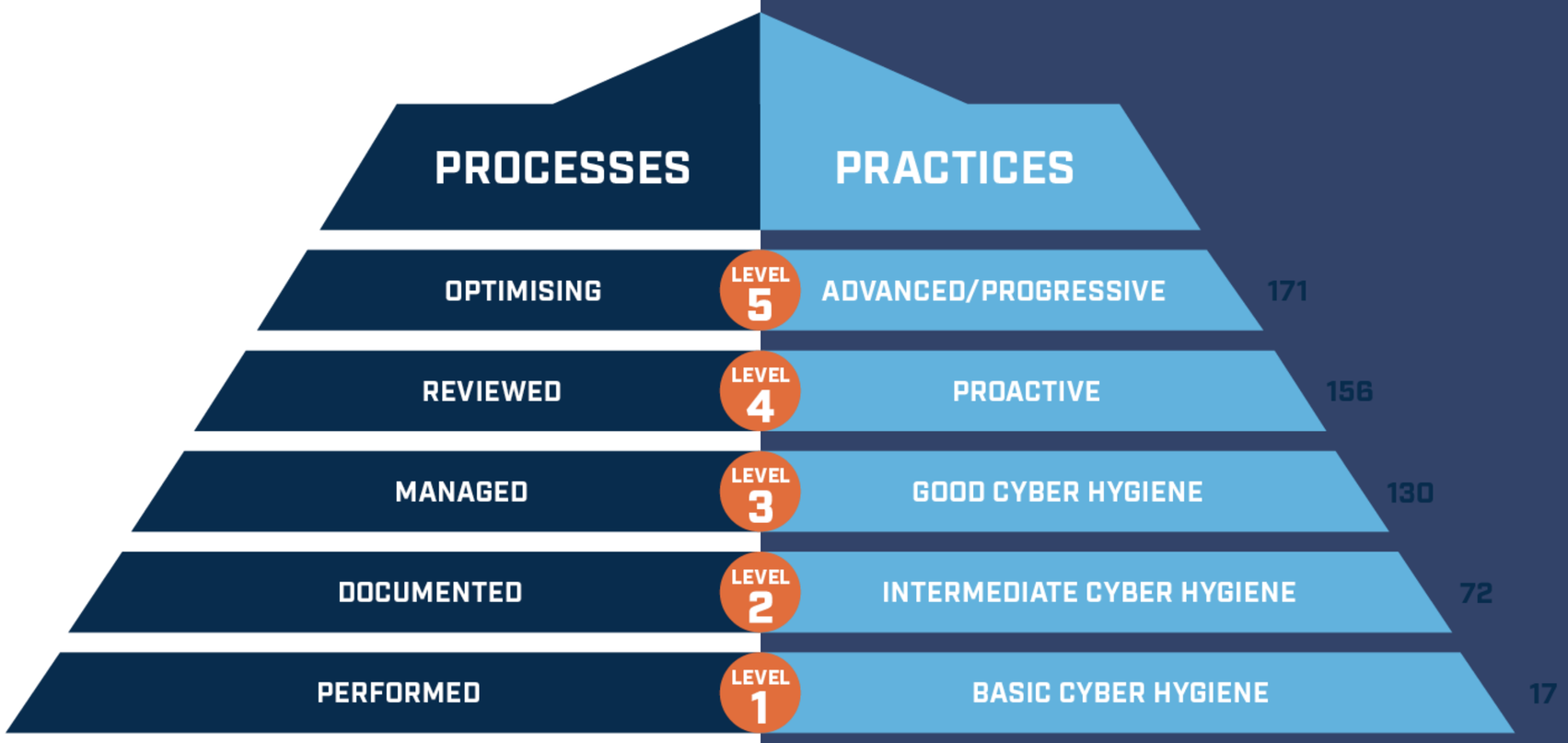
- Level 1: Safeguarding Federal Contract Information (FCI)
- Level 2: Transitioning towards protecting Controlled Unclassified Information (CUI)
- Level 3: Protecting CUI
- Levels 4-5: Protecting CUI and reducing the risk of Advanced Persistent Threats (APTs)

Organizations must demonstrate both the institutionalization of processes and the implementation of practices to achieve a certification level. For example, if an organization demonstrates Level 3 practices but only Level 2 processes, they will be classified overall as Level 2.

CMMC by the numbers

Level 1: 0 processes, 17 practices
Level 2: 2 processes, 55 practices
Level 3: 1 process, 58 practices
Level 4: 1 process, 26 practices
Level 5: 1 process, 15 practices

CMMC levels are cumulative. To achieve Level 5, an organization must demonstrate all 5 processes and 171 practices included in the framework.

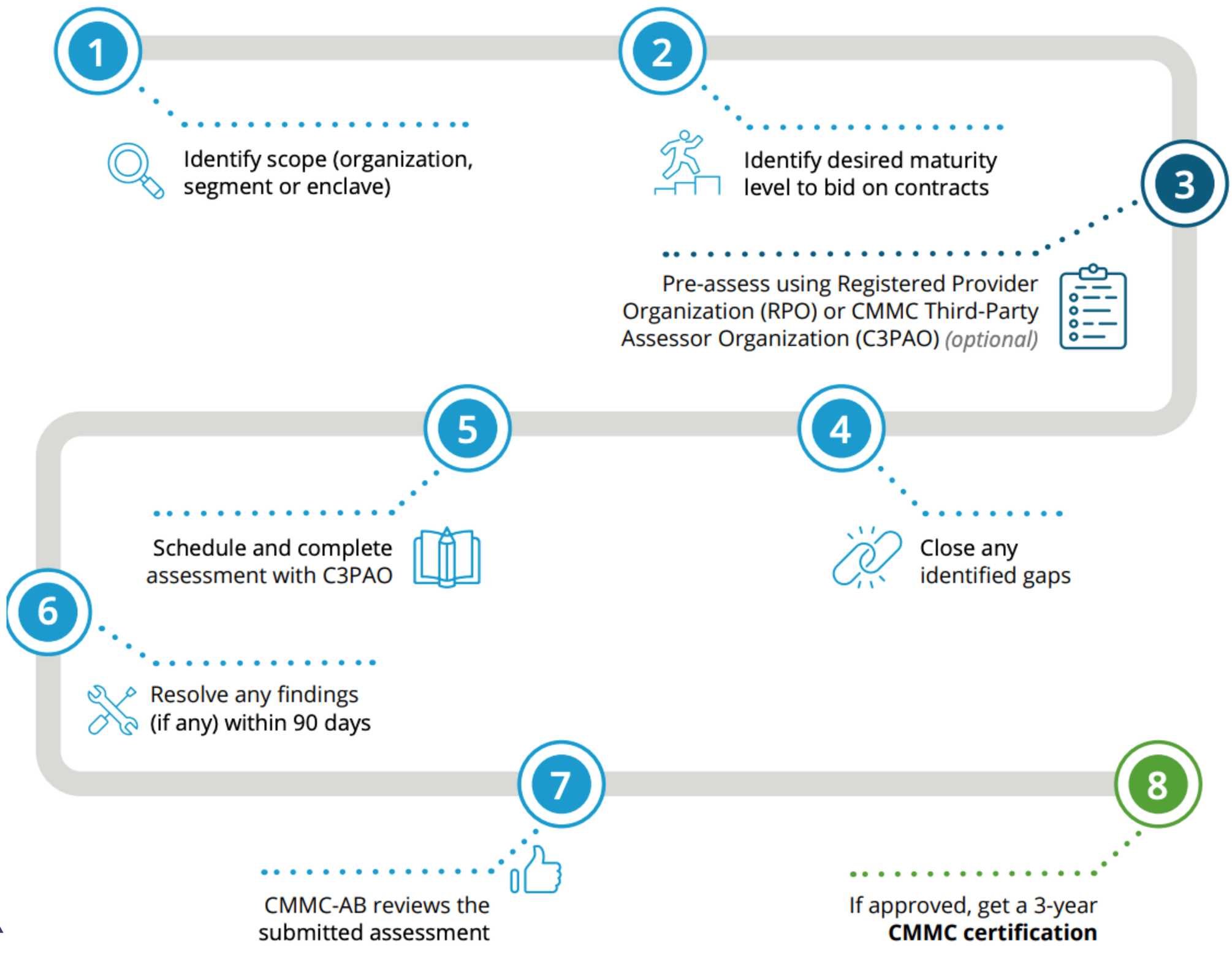


CSG Technologies

Organizations seeking certification (OSC)

CMMC is being incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS), and by 2025 all suppliers will need a certification in order to bid on contracts. Contractors can achieve a CMMC level for their entire enterprise network or for a particular segment or enclave, depending where the protected information is handled and stored. CMMC-AB estimates the certification process will take at least six months.

How to get your organization CMMC certified



CSG Technologies

CMMC assessment overview

CMMC by the numbers

Certified Assessors use the same assessment methods for each contractor. Once a contractor is assessed and certified at a level, other entities (e.g., government sponsors and prime contractors looking to hire subcontractors) have assurance the certified contractor meets CMMC practices and processes.

Methodology the same regardless of size

The CMMC assessment methodology follows a data-centric security process that applies the practices equally, regardless of the contractor's size, constraints or complexity. All CMMC levels are achievable by small, medium and large contractors.

Assessment scope pre-determined by OSC and C3PAO

Prior to a CMMC assessment, the contractor must define the scope for the assessment that represents the boundary for which the CMMC certificate will be issued. Additional guidance on assessment scope will be available in the next version of the CMMC Assessment Guides.

CMMC assessment criteria and methodology

The CMMC assessment procedure is defined in NIST SP 800-171A Section 2.11 and includes:

- **Assessment objects:** Things a Certified Assessor will investigate
- **Assessment actions:** How Certified Assessor will investigate those objects

  Assessment objectives: Determination statement related to the CMMC practice or process being assessed

CMMC assessment objects

Specifications

Document-based artifacts (e.g., policies, procedures, security plans, security requirements, functional specifications, architectural designs) associated with a system.

Mechanisms

The specific hardware, software or firmware safeguards employed within a system.

Activities

The protection-related actions supporting a system that involve people (e.g., conducting system backup operations, exercising a contingency plan and monitoring network traffic).

Individuals

Or groups of individuals, are people applying the specifications, mechanisms or activities described above

CMMC assessment actions

Certified Assessors must select at least two of the three following actions as they collect evidence for each assessment objective:

- **Interviews** tell the Certified Assessor what the contractor staff believe to be true.
- **Documentation** provides evidence of intent.
- **Testing** demonstrates what has or has not been done.

Interview

The Certified Assessor has **discussions with individuals** within an organization to understand if a practice or process has been addressed.

Interviews of applicable staff (possibly at different organizational levels) determine if:

- CMMC practices or processes are implemented
- If adequate resourcing, training and planning have occurred for individuals to perform the practices

Examine

The Certified Assessor can **review, inspect, observe, study or analyze** assessment objects (documents, mechanisms or activities).

Documents need to be in their final forms (drafts are not eligible) and include:

- Policy, process and procedure documents
- Training materials
- Plans and planning documents
- System-level, network and data flow diagrams

Test

The Certified Assessor will determine which practices or objectives within a practice need demonstration or testing. Not all practices will require testing.

For example:
Contractor staff may talk about how users are identified

- Documentation may provide details on how users are identified
- Seeing a demonstration of identifying users provides evidence that the practice is met

CSG Technologies

Assessment findings

The assessment of a CMMC practice or process results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE.

MET: The contractor successfully meets the practice or process.

For each practice or process marked MET, the Certified Assessor includes statements that indicate the response conforms to the objectives and documents the appropriate evidence to support the response.

NOT MET: The contractor has not met the practice or process.

For each practice or process marked NOT MET, the Certified Assessor includes statements that explain why and documents the appropriate evidence that the contractor does not conform to the objectives.

NOT APPLICABLE (N/A): The practice or process does not apply.

For each practice or process marked N/A, the Certified Assessor includes a statement that explains why the practice or process does not apply to the contractor. For example, SC.1.176 might be N/A if there are no publicly accessible systems

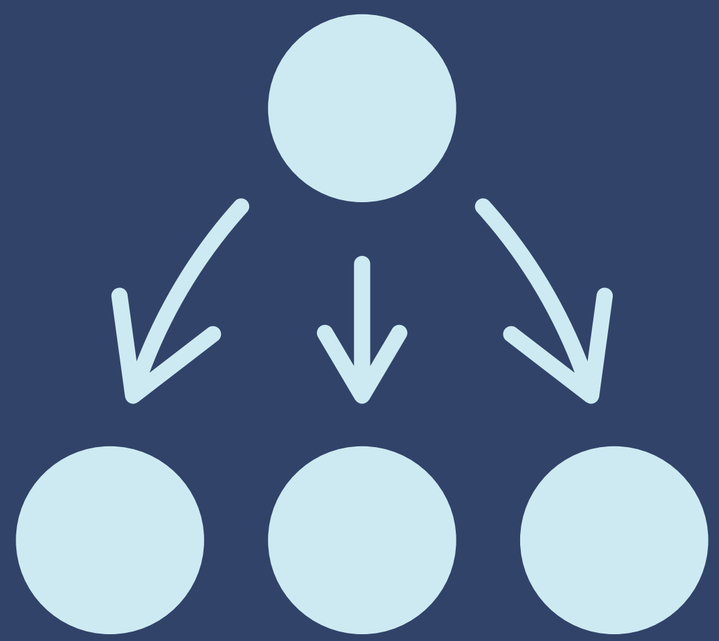
CSG Technologies

Inherited practices

A contractor can inherit practice or process objectives. A practice or process objective that is inherited is met because adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice or process objective.

For each practice or process objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited.

If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice or process.



About US

Based in Jacksonville, FL, CSG Technologies was foundea in i995. Thougn we have a strong connection to the North Florida community, we have a strong North American presence. Though we are technologists, we understand technology exists to enable people to accomplish things beyond their innate abilities and improve the quality of their lives.

CSG
Technologies