AT&T Cybersecurity

AT&T Business

CMMC 2.0: Getting your organization ready for the next-gen Cybersecurity Maturity Model Certification

The Department of Defense (DoD) has taken proactive measures in creating the Cybersecurity Maturity Model Certification (CMMC) to increase cybersecurity standards within the Defense Industrial Base (DIB) and protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)

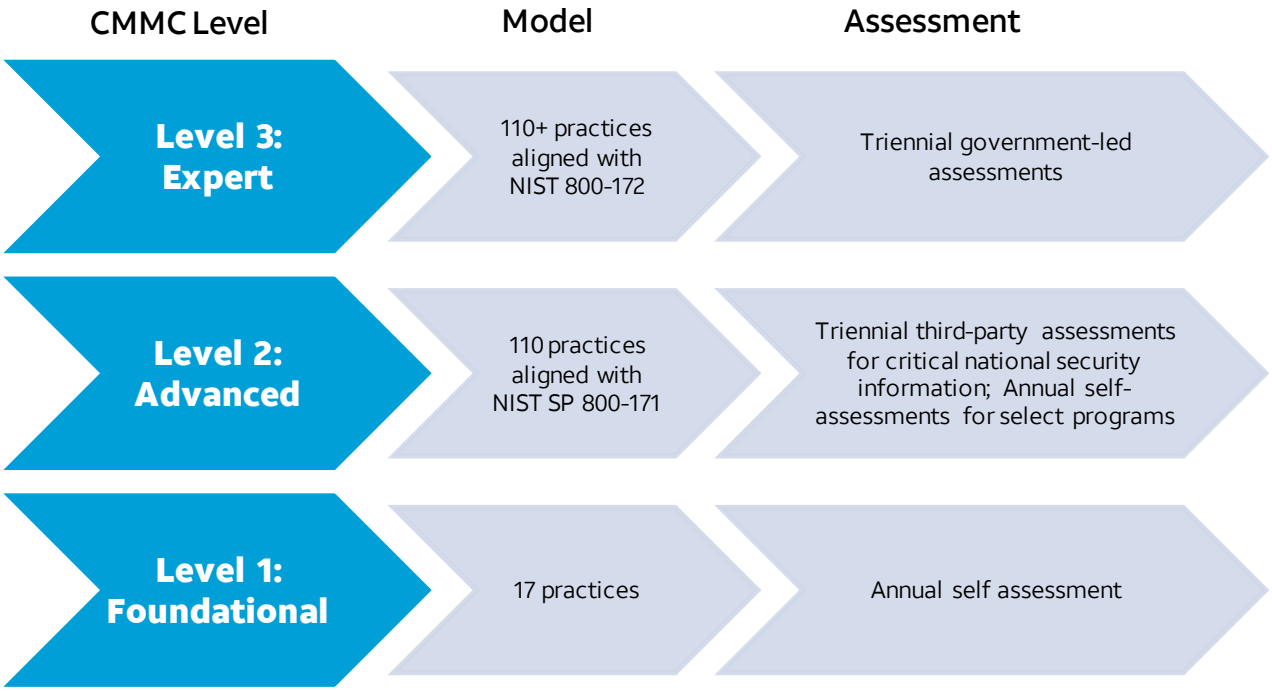
CMMC 2.0, similar to CMMC 1.0, will require companies bidding on defense contracts to meet a certain level of cybersecurity standards when responding to DoD solicitations. CMMC 2.0 levels have been reduced to three levels, from five, to simplify and streamline the process as well as reducing costs to DIB companies.

While you may or may not need to be audited by a certified third-party assessment organization (C3PAO) to attain your certification, you will still need to continue to improve your cybersecurity posture and demonstrate implementation of the requirements. AT&T, as a Registered Provider Organization (RPO), can assist your organization in achieving those requirements through our CMMC Readiness Services.

Potential benefits

- Holistic look to find the practice gaps and process maturity amongst people, process, and technology and to posture against CMMC
- Extensive experience with industry standards and verticals in the DOD supply chain
- Strategic security advisors that can assess, remediate, and provide solutions to meet your desired CMMC level
- Drive faster, more efficient security response

CMMC 2.0 Levels and Assessment Requirements



Importance of picking a trusted registered provider organization (RPO)

If you lack the in-house resources, choosing a cybersecurity strategic partner can help save your organization time in navigating the CMMC model and its required practices and enables confidence in implementing right-sized security solutions. AT&T Cybersecurity can provide the following services:

- **CMMC Scoping**
  - Inventory FCI/CUI Data: Create an inventory of the FCI and CUI data elements found within the CLIENT business enterprise. The inventory includes data elements provided by the federal government as well as those created by the company.
  - *Document CMMC Boundary:* Document the physical and logical boundaries of the CMMC environment that will be subject to certification. Where applicable, recommendation for network architecture changes will be provided to reduce CMMC scope.

- **Gap Assessment**
  - Assess the current state of the information security program to determine the current state of 110 security practices prescribed by CMMC 2.0 Level 2 / NIST 800-171 rev2 and identify missing or unsatisfactory practices. The assessment process includes staff interviews and documentation reviews (processes, procedures, tool-based reports, management dashboards, etc.).

- **Plan of Actions and Milestones (POA&M)** to identify:
  - Issues discovered during a Gap Assessment or current state analysis.
  - Risk level associated with the issue (likelihood of occurrence and impact to business).
  - The tasks and resources necessary to correct the issue.
  - Milestones in completing the tasks.

- **Documentation Development**
  - System Security Plan (SSP): Assist in the development or update of a system security plan (SSP) that satisfies the requirements of CMMC. The SSP describes the characteristics of a system,

including business purpose, system and network architectures, authorized boundaries, data flows and interfaces, and security categorization. In addition, the SSP provides a high-level description of the security controls that have been implemented to satisfy information security requirements.

- *CMMC Domain Policies:* Assist in creating policy statements for each of the 14 CMMC domains. These policies establish the organizations expectations for planning and performing the security activity and communicate those expectations to the entire organization.
- *CMMC Practices:* Assist in drafting or modifying practice narratives or procedures that inform individuals how to perform information security activities in a repeatable manner. Documentation required by CMMC may vary from a desk level procedure to a formal standard operating procedure (SOP).

AT&T Cybersecurity has been providing security services and solutions in the DoD space for many years. We can provide your business with expertise and knowledge as you mature your cybersecurity posture and prepare to meet CMMC. We will provide insights to identify gaps, risks, and solutions to help you work toward certification and get a head start on the competition.

If you are a contractor or vendor planning to do business with the DoD, it is imperative that you work with the right trusted advisor. To learn more about how AT&T Cybersecurity Consulting can prepare your organization to meet CMMC 2.0 standards, visit our website.

AT&T Cybersecurity

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions with advanced technologies (including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™), and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats. Our experienced consultants and Security Operations Center (SOC) analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.