CLOSE SECURITY GAPS BEFORE YOUR CMMC ASSESSMENT

The CMMC was developed to create a framework for uniformly assessing cybersecurity practices in defense industrial base organizations. Using NIST 800-171 as the baseline, the primary objective of CMMC is to secure the Department of Defense supply chain by the application of an enforceable and measurable framework.

Organizations that create Government Off-The-Shelf (GOTS) products, handle Federal Contract Information (FCI), or Controlled Unclassified Information (CUI) will need to show compliance at one of the five levels of the CMMC framework by October of 2025.

BENEFITS

- Eliminate guesswork by working with an expert who understands the intent of the CMMC controls and how they are relevant to your organization
- Gain an overview of your control gaps and a roadmap with a clear path to the most efficient and effective means for meeting those controls
- Improve your team's awareness of CMMC and security in the context of your organization

REDUCE THE UNKNOWNS WITH A PRE-ASSESSMENT

CMMC certification is a pass/fail assessment conducted by an authorized CMMC Third-Party Assessor Organization (C3PAO). If deficiencies are identified, there is a 90-day window to resolve the identified issues. This may or may not be enough time for your organization to close the security gap, depending on your resources and what was discovered. A failed or extended assessment will likely delay certification and could impact your ability to conduct business with the U.S. Government.

The Sirius CMMC Pre-Assessment is designed to help your business evaluate your current environment against the framework, identify weaknesses, and develop a plan to help you mitigate and harden your security posture prior to the certification assessment to help shorten the time to certification.

The CMMC Pre-Assessment is led by a Sirius consultant. Your Sirius team will work your organization's security stakeholders to understand your current system, applications and business environments. This is a collaborative process with open dialogue to help your team develop a strategic roadmap for better security and CMMC compliance.

Focus is on these areas:

- Independent evaluation of your current environment
- Protection of specific information within your system
- 17 domains of the CMMC model
- Collaboration and resolution in preparation for the formal assessment

Your CMMC assessment is not the time to identity security gaps. Sirius will work with you to prepare your organization, security environment and team for a smoother certification assessment. Reach out to your Sirius representative or contact us today to get started.

SIRIUS | SECURITY