Cybersecurity Maturity Model Certification (CMMC) Readiness Assessment

PONDURANCE



The Department of Defense (DOD) has put in place the CMMC 2.0 standard to align stringent cybersecurity processes and practices across the defense industrial base for all defense contractors and subcontractors that handle controlled unclassified information (CUI). As cyber threats continue to evolve, the CMMC framework ensures DOD suppliers have the proper cybersecurity measures in place to protect sensitive information sought after by nation-sponsored attackers and cybercriminals.

Many organizations that do business with the DOD and other government agencies are struggling to meet CMMC requirements. As a registered provider organization, Pondurance is here to help your organization overcome these challenges and guide your way to CMMC 2.0 readiness.

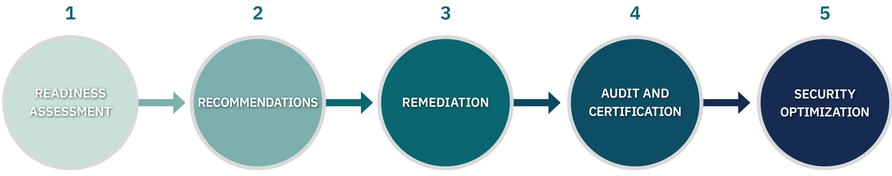
SCOPE

It's important to understand which level of CMMC 2.0 your organization requires. The CMMC Model 2.0 has three distinct levels of certification to ensure that each defense contractor working with the DOD has the required cybersecurity measures in place to protect sensitive information.

LEVEL	1	2	3
PROCESSES	BASIC CYBER HYGIENE	ADVANCED CYBER HYGIENE	EXPERT CYBER HYGIENE
PRACTICES	• Any supplier contracting with the DOD will require Level 1 certification. • 17 Practices • Annual self-assessment	• Required by the majority of DOD acquisitions. • 100 practices aligned with NIST SP 800-171 • Triennial 3rd-party assessments for critical national security information • Annual self-assessment for select programs	• Limited organizations handle the type of data for the Expert Level (3). • 110+ practices based on NIST SP 800-172 • Triennial government-led assessments

CMMC READINESS ASSESSMENT

CMMC 2.0 has three distinct levels of certification to ensure that each defense contractor working with the DOD has the required cybersecurity measures in place to protect sensitive information. It's important to understand which level applies to your organization and to be prepared for certification as well as assessment. Our CMMC readiness assessment has five steps to assist.



READINESS ASSESSMENT	RECOMMENDATIONS	REMEDIATION	AUDIT AND CERTIFICATION	SECURITY OPTIMIZATION
Pondurance identifies any deficiencies across all relevant CMMC domains and related processes, capabilities, and practices.	Pondurance provides you with recommendations based on our skilled registered practitioners that have years of experience auditing and identifying security gaps.	As part of the remediation phase, we offer the option of staff augmentation if desired.	Work directly with a Pondurance CMMC third-party assessor organization partner or a third-party assessor of your choice.	Ongoing security protection is critical to continually protect CUI. A well-documented plan and 24/7 detection and response can help you maintain your certification.

If additional resources are needed, we also offer Pondurance Managed Detection and Response services, a comprehensive Vulnerability Management Program, and Incident Response.

Contact Pondurance for Your CMMC Assessment Today!

pondurance.com

Copyright © 2022 Pondurance