Begin Your CMMC Journey with an Authorized Kratos CMMC 2.0 Assessment

KRATOS
READY FOR WHAT'S NEXT™

As a CMMC Third Party Assessment Organization (C3PAO), Kratos teams are ready to conduct the CMMC assessments that are a prerequisite to CMMC 2.0 certification. The assessment process consists of three phases and, depending on complexity, most assessments will be completed in four to six weeks. Much of the progress Organizations Seeking Certification and DIB members have taken will still apply and ease CMMC 2.0 certification. CMMC 2.0 still addresses security concerns related to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) and divides certification levels based on what type of information an organization handles. CMMC 2.0 does not alter the Level 1 controls, but only requires a self-attestation for Level 1 certification. Certified C3PAOs are still able to assess or offer advisory services.

Phase 1: Preparation

Analyze Requirements
Outline the assessment request and present the assessment team.

Develop Assessment Plan
Determine Certification Level target and the boundary of the assessment, including locations, dates and general timing.

Verify Assessment Readiness
Review assignment logistics, risk status, feasibility, objective evidence readiness and assessment team readiness

Phase 2: Assessment

Collect/Examine Objective Evidence (OE)
The assessment team collects artifacts, conducts interviews and observes demonstrations.

Rate Practices/Validate Results
The evidence will be reviewed for adequacy and sufficiency. Based on those findings, the team will recommend a pass/fail rating.

Generate Final Results
The assessment team aggregates all ratings. If there are outstanding findings, the team can initialize the remediation phase.

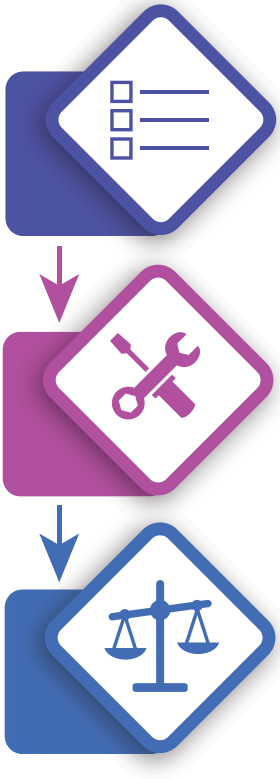
Phone: 703.254.2016 • EMail: CyberSales@KratosDefense.com • Web: www.KratosDefense.com

Phase 3: Report Findings Phase

The assessment team presents the final results package to the organization seeking certification (OSC) including the ML was achieved/not achieved, practice ratings, daily report logs, and the potential for remediation. The C3PAO submits the results to the AB for review or remediation request confirmation.

Phase 4: Remediation

If issues are identified in the Report Findings phase, a Remediation phase can be initiated to evaluate remedial actions taken.



Identify Remediation Approach

Outline the assessment request and present the assessment team.

Execute Remediation

Outline the assessment request and present the assessment team.

Assessment Adjudication

Outline the assessment request and present the assessment team.

Begin Your CMMC Journey Here.

Rely on Kratos for your CMMC Compliance Efforts

Kratos has years of robust compliance and certification experience with government and commercial standards requirements. These now include the Cybersecurity Maturity Model Certification 2.0 (CMMC) along with the Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry (PCI), Federal Information Security Management Act (FISMA) and the National Institute of Standards & Technology (NIST)/Risk Management Framework (RMF). Kratos is viewed as a trusted compliance and governance partner by the Department of Defense (DoD), Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations. Kratos cybersecurity services include Compliance, Governance, Risk Management & Strategy and Cyber: Operations, Defense, & Engineering services.