ACCESS ONE

CMMC 2.0 PROCESS ROADMAP

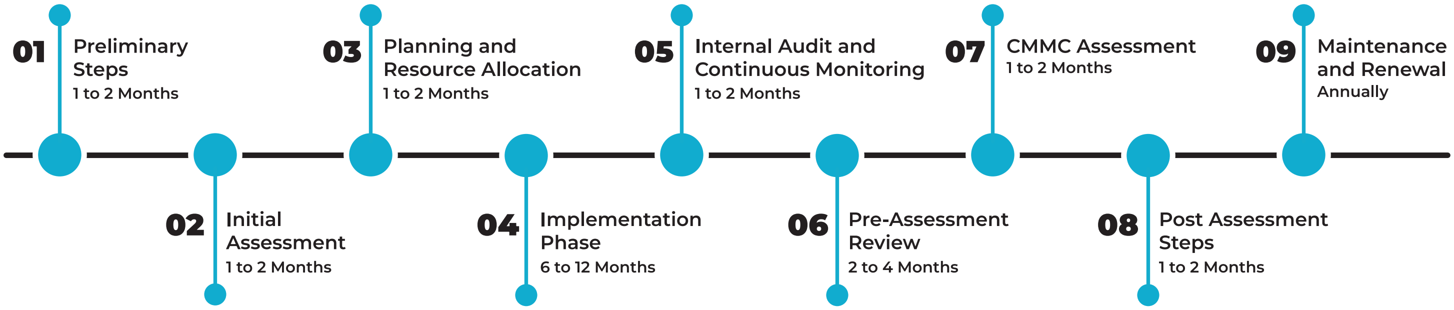
Revision June 2025

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

www.accessoneinc.com | (800) 804-8333
820 W. Jackson Blvd | 6th Floor | Chicago, IL 60607

Introduction

Becoming Cybersecurity Maturity Model Certification (CMMC 2.0) certified involves a comprehensive and structured approach to ensure compliance with the Department of Defense (DOD) cybersecurity requirements. The CMMC 2.0 Framework was released early in 2024 and applies to any entity producing products designed for or customized for the DOD. Below is a detailed outline of the steps a company should take to achieve CMMC 2.0 certification:



01 Preliminary Steps
1 to 2 Months

02 Initial Assessment
1 to 2 Months

03 Planning and Resource Allocation
1 to 2 Months

04 Implementation Phase
6 to 12 Months

05 Internal Audit and Continuous Monitoring
1 to 2 Months

06 Pre-Assessment Review
2 to 4 Months

07 CMMC Assessment
1 to 2 Months

08 Post Assessment Steps
1 to 2 Months

09 Maintenance and Renewal
Annually

CMMC 2.0 OUTLINE VISUAL

01 Preliminary Steps 1 - 2 Months

Understand CMMC Requirements:
· Determine which level of certification is required based on your contract needs.
· Familiarize with the CMMC model and practices required at each level.

Executive Buy In:
Secure support from senior management for the resources and commitment needed for CMMC compliance.

02 Intial Assessment 1 - 2 Months

Gap Analysis:
· Conduct a self-assessment or hire a consultant to perform a gap analysis against the CMMC requirements for the desired level.
· Identify current cybersecurity posture and areas that need improvement.

Documentation Review:
Review existing cybersecurity policies, procedures, and documentation.

03 Planning and Resources Allocation 1 - 2 Months

Develop a Plan of Action and Milestones (POA&M):
· Create a detailed plan to address gaps identified during the assessment.
· Establish timelines, responsible parties, and milestones for remediation efforts.

Allocate Resources:
Allocate necessary financial, technological, and human resources to implement the POA&M.

04 Implementation Phase 6 - 12 Months

Policy and Procedure Development:
Develop or update cybersecurity policies and procedures to meet CMMC requirements.

Training and Awareness:
Conduct training programs to ensure all employees are aware of and adhere to new cybersecurity practices.

Technical Controls Implementation:
Implement required security controls (e.g., access controls, incident response plans, encryption, multifactor authentication).

System and Network Changes:
Make necessary changes to IT systems and network architecture to comply with CMMC standards.

05 Internal Audit and Continous Monitoring 1 - 2 Months

Conduct Internal Audits:
Perform regular internal audits to ensure that implemented controls are functioning correctly and policies are being followed.

Continuous Monitoring:
Establish continuous monitoring mechanisms to track security controls and detect potential threats in real-time.

06 Pre-Assessment Review 2 - 4 Months

Mock Assessment:
Conduct a mock assessment with a third-party consultant to identify any remaining gaps.

Continuous Monitoring:
Establish continuous monitoring mechanisms to track security controls and detect potential threats in real-time.

07 CMMS Assessment 1 - 2 Months

Select a C3PAO:
Choose a Certified Third-party Assessment Organization (C3PAO) authorized by the CMMC Accreditation Body (AB) to conduct the formal assessment.

Prepare for Assessment:
· Gather all necessary documentation and evidence of compliance.
· Ensure key personnel are available to assist during the assessment process.

Undergo Assessment:
· Participate in the formal assessment conducted by the C3PAO.
· Respond to any queries and provide additional information as requested by the assess

08 Post Assessment Steps 1 - 2 Months

Receive Assessment Results:
Review the assessment report provided by the C3PAO.

Address Deficiencies:
If any deficiencies are identified, address them promptly and submit evidence of remediation.

Certification Award:
Upon successful completion of the assessment and remediation, receive CMMC certification for the specified level.

09 Maintenance and Renewal Annually

Continuous Improvement:
Continuously improve cybersecurity practices and controls.

Ongoing Compliance:
Maintain compliance with CMMC requirements through regular updates and monitoring.

Renewal Process:
Plan for periodic reassessments to maintain certification as required by the DoD (typically every three years).

ACCESS ONE