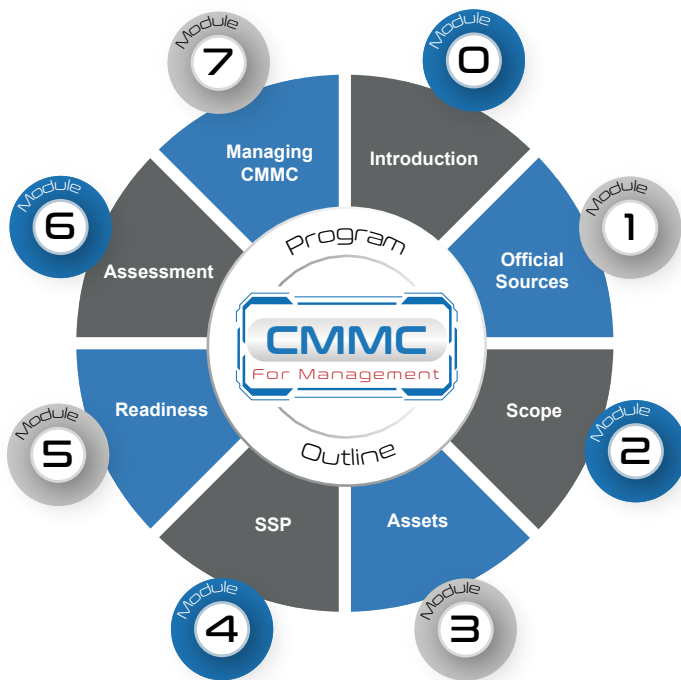


Summary

- Understand and manage Cybersecurity Maturity Model Certification (CMMC) requirements for protecting FCI and CUI environments.
- Prepare organizations for CMMC readiness reviews, assessments, and certification activities.
- Support ongoing cybersecurity compliance management and continuous improvement efforts.

Program Outline



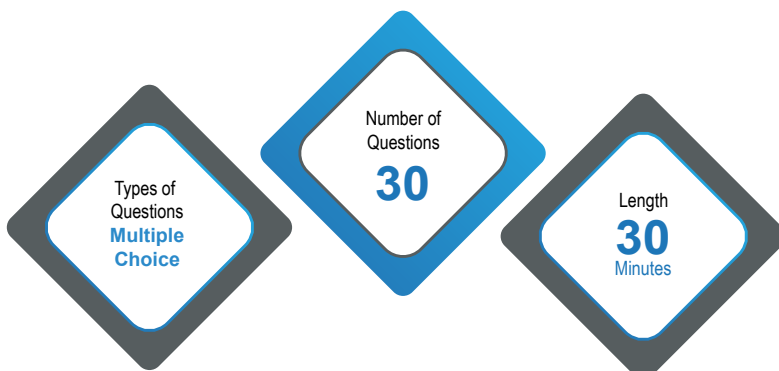
Learning Objectives

- Identify and use official CMMC guidance for implementation and assessment.
- Define scope by locating systems and assets handling CUI.
- Map assets to systems and workflows for compliance readiness.
- Create and maintain an SSP detailing control implementation and responsibilities.
- Prepare and present evidence to demonstrate control implementation during assessment.

Intended Audience

- Executives and senior leadership
- CISOs and cybersecurity managers
- Compliance and governance teams
- IT and security management personnel
- Program and contract managers
- Defense contractors and subcontractors
- Organizations preparing for CMMC assessments

Exam Specifications



Module Exam Weight

#	Domain	Exam Weight
0	Introduction	10%
1	Official Sources	10%
2	Scope	20%
3	Assets	15%
4	SSP	20%
5	Readiness	10%
6	Assessment	10%
7	Managing CMMC	5%



Module 0 Introduction

- Overview of the CMMC framework and certification structure.
- Understanding FCI, CUI, and DoD cybersecurity expectations.
- Introduction to the CMMC ecosystem and terminology.
- Business impact of CMMC on defense contractors.
- Overview of assessment types and certification pathways.

Module 1 Official Sources

- Understanding official CMMC guidance and documentation.
- Review of CMMC Assessment Guides, Scoping Guides CMMC Assessment Process (CAP) and NIST SP 800-171 / 171A / 172
- Using authoritative resources for compliance preparation.
- Understanding regulatory references and assessment expectations.

Module 2 Scope

- Defining the CMMC assessment boundary.
- Identifying systems that process, store, or transmit CUI.
- Understanding in-scope vs out-of-scope assets.
- Mapping CUI data flows across environments.
- Scoping considerations for cloud, remote, and hybrid systems.
- Managing ESP and CSP scoping requirements.

Module 3 Assets

- Classification of CMMC asset categories.
- Asset inventory and ownership requirements.
- Understanding asset relationships and dependencies.
- Documentation expectations within the SSP.
- Risk-based asset management concepts.

Module 4 SSP

- Developing and maintaining the System Security Plan.
- Defining system boundaries and environments.
- Mapping controls to NIST SP 800-171 requirements.
- Documenting implementation methods and responsibilities.
- Managing diagrams, inventories, and inherited controls.
- Common SSP gaps and assessment challenges.

Module 5 Readiness

- Preparing for CMMC assessments and readiness reviews.
- Organizing evidence, policies, and procedures.
- Understanding assessment artifacts and traceability.
- Identifying readiness gaps and remediation activities.
- Preparing personnel for interviews and testing activities.
- Managing POA&Ms and operational plans of action.

Module 6 Assessment

- Understanding the CMMC assessment lifecycle.
- Overview of assessment phases .
- Assessment scoring methodology (MET, NOT MET & N/A)
- Examine, Interview, and Test assessment methods.
- Assessment sampling and quality assurance activities.
- Out-briefs, reporting, appeals, and certification issuance.

Module 7 Managing CMMC

- Sustaining ongoing CMMC compliance.
- Governance and executive oversight responsibilities.
- Managing annual affirmations and periodic assessments.
- Maintaining SSPs, inventories, and evidence repositories.
- Continuous monitoring and compliance improvement.
- Managing certification renewals and organizational readiness.

