CMMC 2.0 For Dummies

2W Technologies, INC.

CMMC 2.0 Executive Overview

A practical guide for defense contractors preparing for compliance

Executive Summary

- CMMC 2.0 is now a business requirement for defense contractors that manage FCI or CUI.
- Most organizations should focus on Level 1 if they manage FCI only or Level 2 if they manage CUI.
- Level 2 requires a demonstrable security program aligned to NIST SP 800-171.
- 2W Technologies support the technical foundation, evidence, and secure cloud environment needed for readiness.

What is CMMC 2.0?

CMMC 2.0 is the Department of Defense cybersecurity certification framework for contractors that manage sensitive defense information. It is designed to ensure organizations can adequately protect Federal Contract Information and Controlled Unclassified Information before they are awarded or retain applicable DoD contracts.

- It protects two main types of data:
    - FCI (Federal Contract Information) – contract-related information that is not intended for public release.
    - CUI (Controlled Unclassified Information) – sensitive technical, operational, or program information that requires defined safeguards.

The model has three levels, but most suppliers should focus on Level 1 or Level 2 based on whether they manage FCI only or CUI.

The Three CMMC Levels

Level	Applies To	Requirement	Assessment Type	Business Impact
Level 1	FCI only	17 basic safeguarding requirements	Annual self-assessment	Baseline eligibility for lower-risk work
Level 2	**CUI**	**110 NIST SP 800-171 requirements**	**Third-party assessment in most cases**	**Primary requirement for most defense suppliers managing CUI**
Level 3	Specialized, high-priority programs	Level 2 plus additional requirements	Government assessment	Advanced requirement for select programs

Level 2 is the primary requirement for organizations that manage CUI in support of defense contracts.

Level 1 vs. Level 2: Key Distinction

- Level 1: Basic safeguarding requirements for organizations that manage FCI only. Assessment is typically self-reported.
- Level 2: A more rigorous security program for organizations that manage CUI, often requiring independent third-party assessment.

Source of the Level 2 Requirements

Level 2 maps to the 110 security requirements in NIST SP 800-171. These requirements are organized into 14 control families:

People Controls	Process Controls	Technology Controls
• Awareness & Training • Personnel Security • Physical Protection	• Audit & Accountability • Incident Response • Maintenance • Risk Assessment • Security Assessment	• Access Control • Configuration Management • Identification & Authentication • Media Protection • System & Communications Protection • System & Information Integrity

Path to Level 2 Certification

1. Scope	Confirm whether CUI is present and define the assessment boundary.
2. Gap Assess	Evaluate the current environment against Level 2 requirements.
3. Remediate	Implement missing controls, document evidence, and close priority gaps.
4. Assess	Engage a C3PAO when required and complete the official assessment.
5. Maintain	Sustain evidence, annual affirmations, and ongoing compliance discipline.

Incident reporting: Serious cyber incidents must be reported to the DoD within 72 hours.

Scoping Strategy

Scoping defines which systems, users, and processes are included in the assessment boundary. A well-designed CUI enclave can reduce cost and complexity by isolating sensitive work into a controlled environment while keeping unrelated systems outside the audit scope.

The Shared Responsibility Model

Successful CMMC readiness depends on clear division of responsibility across the cloud provider, MSP, and contractor organization.

Microsoft / Cloud Provider	2W Technologies	Client Organization
Provides the compliant infrastructure foundation, including cloud platform capabilities and underlying service controls.	Designs, deploys, and manages the secure cloud environment, identity controls, monitoring, backups, and related technical safeguards.	Owns policies, training, physical security, HR processes, governance, and final compliance accountability.

2W provides a Shared Responsibility Matrix that defines ownership across the client, 2W, and Microsoft.

2W Technologies Client Support

- Design and deploy secure GCC High cloud environments.
- Configure MFA, firewalls, encryption, logging, backups, and related technical controls.
- Provide technical evidence, diagrams, and documentation for assessor review.
- Support scoping, technical remediation, and environment readiness.
- Participate in assessments to address technical questions within 2W's scope of responsibility.

Client-Owned Responsibilities

- Company policies and governance documentation.
- Security awareness training and role-based training.
- Physical facility security.
- POA&M ownership and remediation governance.
- HR processes, including screening and offboarding.

Recommended Next Steps

1. Confirm whether the organization manages CUI.
2. Define the assessment scope and evaluate whether a CUI enclave is appropriate.
3. Complete a readiness or gap assessment.
4. Remediate technical gaps with 2W or another qualified technical partner.
5. Address policies, training, HR, and physical security internally or with a compliance advisor.
6. Conduct a mock assessment before engaging a C3PAO.
7. Schedule the official C3PAO assessment when ready.
8. Maintain evidence, affirmations, and ongoing compliance discipline after certification.

Recommended Action

Recommended Action: Determine whether CUI is in scope, define the assessment boundary, and complete a readiness assessment before engaging a C3PAO.