CMMC Level 2—Understanding the 14 Security Domains

NIST SP 800-171

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) Level 2 ensures organizations protect Controlled Unclassified Information (CUI) when working with the U.S. Department of Defense.

It is based on 110 security requirements from NIST SP 800-171, organized into 14 domains.

Access Control (AC)

Who can access systems and data and what they can do.
Limits access to only authorized users and enforces least privilege.

Awareness & Training (AT)

Making sure people know how to stay secure.
Security training helps users recognize threats like phishing.

Audit & Accountability (AU)

Tracking what happens on systems.
Logs activity so suspicious actions can be detected and investigated.

Configuration Management (CM)

Keeping systems securely configured.
Prevents unauthorized or risky system changes.

Identification & Authentication (IA)

Proving who you are.
Uses unique user IDs, strong passwords, and MFA.

Incident Response (IR)

What to do when something goes wrong.
Requires plans to detect, report, and recover from cyber incidents.

Maintenance (MA)

Securing system maintenance activities.
Controls how systems are serviced, especially remote maintenance.

Media Protection (MP)

Protecting data on physical and digital media.
Covers USBs, backups, and proper media disposal.

Personnel Security (PS)

Reducing insider risk.
Ensures access is removed when employees leave or change roles.

Physical Protection (PE)

Protecting buildings, rooms, and equipment.
Limits physical access to systems and facilities.

Risk Assessment (RA)

Knowing what could go wrong.
Identifies vulnerabilities and cybersecurity risks.

Security Assessment (CA)

Proving security controls are in place.
Includes self-assessments, documentation, and improvement plans.

System & Communications Protection (SC)

Protecting networks and data in transit.
Uses encryption, firewalls, and network boundaries.

System & Information Integrity (SI)

Keeping systems clean and trustworthy.
Detects malware, applies patches, and monitors for threats.