Defense and Compliance

ComplyClinic Playbook

CMMC Readiness Playbook for Small Defense Contractors

A plain-English guide to preparing for CMMC by organizing scope, evidence, and practical security controls.

Audience: Small manufacturers, engineering firms, suppliers, and service providers supporting DoD work.

General educational resource only. This is not legal advice, certification advice, or a substitute for a formal security risk analysis, CMMC assessment, or incident response engagement.

CMMC readiness starts with scoping

Start by identifying whether your work involves Federal Contract Information, Controlled Unclassified Information, or both. The type of information drives the expected protection level and assessment path.

Do not start by buying tools. Start by understanding where covered information lives, who accesses it, and how it moves.

FCI and CUI in practical terms

FCI is information provided by or generated for the government under a contract that is not intended for public release. CUI is more sensitive and requires stronger protection.

Common locations include email, file shares, engineering folders, ERP systems, cloud storage, help desk tickets, supplier portals, laptops, and backups.

Network segmentation and DMZ concepts

Public-facing systems should be isolated from internal systems that store sensitive business, FCI, or CUI data. A DMZ can reduce risk by separating internet-exposed services from trusted internal networks.

For small contractors, segmentation does not have to be overbuilt. Start with simple zones: users, servers, guest Wi-Fi, IoT, management, and externally facing services.

Microsoft 365 and identity controls

Identity is often the control plane. Enforce MFA, conditional access, least privilege, logging, external sharing controls, and secure device access.

Review whether standard commercial cloud settings are sufficient for your contract needs. Some environments may require GCC High or other controlled configurations depending on CUI requirements.

Evidence matters

CMMC readiness is not only about doing security work. It is about proving it. Keep policies, procedures, screenshots, configuration exports, training records, access reviews, incident logs, and system security plan artifacts.

If a control is implemented but undocumented, it may still create assessment pain.

Common mistakes

Skipping scoping, assuming IT vendors handle everything, keeping CUI in normal email, ignoring subcontractor flow-downs, using shared accounts, lacking logs, and treating policy templates as implementation.

90-day readiness roadmap

Days 1-30: scope FCI/CUI and identify systems. Days 31-60: close identity, endpoint, and backup gaps. Days 61-90: build evidence, update policies, and prepare a remediation roadmap.

Next step: Book a CMMC readiness overview to map your environment, contracts, and evidence gaps. Schedule now

Need help turning this into a practical roadmap? Book a free consultation at complyclinic.com.

ComplyClinic • Practical cybersecurity, compliance readiness, automation, app development, and AI governance support.