TECBOMO LLC

CMMC Readiness Checklist

A Strategic Framework for Reducing Complexity & Eliminating Supply Chain Bottlenecks

> **Pre-Audit Operational Guide: Aligning NIST SP 800-171 Controls with Department of Defense (DoD) Supply Chain Prerequisites.**

Achieving Cybersecurity Maturity Model Certification (CMMC) requires a flawless convergence of technical control engineering, network boundaries, and verifiable documentation. This checklist serves as an operational baseline to evaluate your organization's technical and administrative posture before scheduling a formal third-party audit.

1. Boundary Scoping & Architecture Optimization

Before deploying technical controls, organizations must strictly define where Controlled Unclassified Information (CUI) lives, flows, and rests. Restricting your boundary limits compliance costs and infrastructure overhead.

☐	Milestone Item	Operational Technical Objective	*Audit Artifact Source*
☐	Data Flow Mapping	Trace all ingest, storage, processing, and egress points for CUI across your network environment.	Data Flow Diagram
☐	Enclave Isolation	Isolate corporate infrastructure from the CUI environment using logical or physical firewalls to limit assessment scope.	Network Topology Map
☐	Asset Categorization	Classify all connected assets into CUI Assets, Security-Protection Assets, Out-of-Scope Assets, or CRMA.	Asset Inventory Log

2. Technical Control Implementation (NIST SP 800-171 Core)

These core technical domains present the highest frequency of failure during official C3PAO reviews. Security systems must function seamlessly without paralyzing regular business velocity.

☐	Milestone Item	Operational Technical Objective	*Audit Artifact Source*
☐	Access Control (AC)	Enforce the Principle of Least Privilege. Restrict system access to explicitly authorized users and automated processes.	Active Directory Group Policy
☐	Identity & Auth (IA)	Deploy Multi-Factor Authentication (MFA) for all local, network, and remote administrative access sessions.	MFA Configuration Profile

☐	Milestone Item	Operational Technical Objective	*Audit Artifact Source*
☐	Audit & Account (AU)	Establish system logging that tracks user actions to ensure accountability. Archive records for forensic inspection.	SIEM Log Repositories
☐	Media Protection (MP)	Sanitize or physically destroy digital media containing CUI before disposal or release for reuse.	Media Destruction Logs
☐	System Comm (SC)	Implement FIPS 140-validated cryptographic modules to protect CUI during digital transmission.	TLS/VPN Cipher Suite Specs

Critical Supply Chain Integrity Note

TECBOMO maintains an uncompromising stance on defensive infrastructure authenticity. Per federal sourcing mandates, all hardware tokens, cryptographic elements, and computing units utilized within your CUI environment must maintain a verifiable chain of custody. **Refurbished or unverified third-party components are strictly prohibited.**

3. Institutional Governance & Documentation Lifecycle

An organization cannot pass an audit on technical controls alone. Governance processes must prove that cybersecurity protocols are deeply institutionalized, documented, and continuously managed.

☐	Milestone Item	Operational Technical Objective	*Audit Artifact Source*
☐	System Security Plan	Maintain a live, comprehensive System Security Plan (SSP) describing operational boundaries and control implementations.	Approved SSP Document
☐	POA&M Management	Document deficiency plans within a Plan of Action and Milestones (POA&M) with explicit remediation dates.	Active POA&M Log
☐	Incident Response (IR)	Develop and test incident handling capabilities, including mandatory 72-hour reporting thresholds to the DIBNet portal.	IR Plan & IRP Test Results

Stalled by Documentation Bottlenecks or Scoping Friction?

Don't let compliance paralysis disrupt your defense contract pipeline. TECBOMO humanizes technical architecture, streamlining your path to CMMC verification. Contact our federal contract security team to schedule an optimized boundary scoping session.