CMMC Level 1: Self-Assessment Checklist

Published by: CyberSec Insight

Version: 2.0 (Self-Assessment Guide)

Scope: Basic Safeguarding of Federal Contract Information (FCI)

Executive Overview

Level 1 of the Cybersecurity Maturity Model Certification (CMMC) consists of **15 security requirements** derived directly from FAR Clause 52.204-21. To achieve compliance, an organization must perform an annual self-assessment and upload the results to the Supplier Performance Risk System (SPRS).

Domain 1: Access Control (AC)

ID	Requirement	Compliance Task	Status
3.1.1	Authorized User Control	Create a master list of all users and hardware devices. Disable all inactive accounts.	[ ]
3.1.2	Transaction/Function Control	Limit user permissions to only what is necessary for their job (Role-Based Access Control).	[ ]
3.1.20	External System Connections	Restrict the use of unauthorized USBs, personal laptops, or public cloud storage for FCI.	[ ]

3.1.22	Public Content Control	Review all website and social media content to ensure no sensitive contract data is exposed.	[ ]

Domain 2: Identification & Authentication (IA)

ID	Requirement	Compliance Task	Status
3.5.1	Identifier Management	Ensure every person on the network has a unique, traceable ID (No shared logins).	[ ]
3.5.2	Authenticator Management	Enforce strong password policies and use Multi-Factor Authentication (MFA) for all users.	[ ]

Domain 3: Media Protection (MP)

ID	Requirement	Compliance Task	Status
3.8.3	Media Sanitization	Implement a "Wipe or Shred" policy for old hard drives and physical documents containing FCI.	[ ]

Domain 4: Physical Protection (PE)

ID	Requirement	Compliance Task	Status
3.10.1	Physical Access Control	Secure the office perimeter. Lock server closets and ensure workstations are not visible to the public.	[ ]
3.10.3	Visitor Control	Require all visitors to sign in and be escorted by an authorized employee at all times.	[ ]
3.10.4	Physical Access Logs	Maintain a physical logbook or digital badge record of everyone entering the facility.	[ ]
3.10.5	Physical Device Control	Maintain an inventory of all physical keys, fobs, and badges issued to staff.	[ ]

Domain 5: System & Communications Protection (SC)

ID	Requirement	Compliance Task	Status
3.13.1	Boundary Protection	Verify that a firewall is active and that your network has a clear "Inside" and "Outside" boundary.	[ ]
3.13.5	Network Separation	Ensure your Guest Wi-Fi is logically separated from the network where FCI is stored.	[ ]

Domain 6: System & Information Integrity (SI)

ID	Requirement	Compliance Task	Status
3.14.1	Flaw Remediation	Enable automatic updates for Windows/macOS and all critical software to patch vulnerabilities.	[ ]
3.14.2	Malicious Code Protection	Deploy Antivirus/Endpoint Protection on all workstations and servers.	[ ]
3.14.4	Update Protection	Configure antivirus software to update definitions automatically every day.	[ ]
3.14.5	System Scanning	Perform weekly full-system scans and real-time scanning for all downloads.	[ ]

CyberSec Insight Professional Tip

> **Evidence is King.** Simply checking the box isn't enough for a true audit. For every "Yes" on this list, your organization should have a corresponding screenshot, policy document, or log file to prove the control is active.