https://www.onsite-tech.com
Email: info@onsite-tech.com
Info: 602-595-2227

CMMC Readiness Checklist

This self-assessment checklist is designed to help your organization assess where it currently stands in relation to the 14 CMMC 2.0 domains. Use it to identify areas where you're aligned—and where further attention may be needed to meet the requirements outlined in the CMMC 2.0 Final Rule.

1. Access Control (AC)

Controls who can access sensitive systems and data.

- ☐ Maintain role-based access controls for users
- ☐ Enforce Multi-Factor Authentication (MFA)
- ☐ Assign unique credentials to each user
- ☐ Disable unused accounts promptly
- ☐ Restrict remote access and use VPNs or other secure methods
- ☐ Implement session timeouts for inactive users
- ☐ Apply Least Privilege principles
- ☐ Limit CUI flow and control mobile device access

2. Awareness and Training (AT)

Equip your team to recognize and respond to security threats.

- ☐ Provide annual cybersecurity awareness training
- ☐ Train users to spot phishing and social engineering
- ☐ Test employee readiness with simulated attacks
- ☐ Track training completion and effectiveness
- ☐ Include insider threat training and role-based modules

3. Audit and Accountability (AU)

Tracks activity on systems to detect and investigate anomalies.

- ☐ Log all user access to systems and data
- ☐ Retain audit logs for required periods
- ☐ Review logs regularly for suspicious activity
- ☐ Investigate and respond to anomalies
- ☐ Assign responsibility for audit log review

4. Configuration Management (CM)

Reduces vulnerabilities by enforcing secure system settings

- ☐ Implement standardized configuration baselines
- ☐ Harden operating systems and applications
- ☐ Track and document all configuration changes
- ☐ Monitor for unauthorized modifications
- ☐ Apply Least Functionality principle (disable unused services)
- ☐ Use Automated Configuration Monitoring tools

5. Identification & Authentication (IA)

Verifies users before granting access.

- ☐ Require unique user IDs for all access
- ☐ Enforce strong password policies
- ☐ Require periodic password changes
- ☐ Lock accounts after failed login attempts
- ☐ Use digital certificates or smart cards where feasible

6. Incident Response (IR)

Defines how you detect, report, and recover from cybersecurity incidents.

- ☐ Maintain a documented Incident Response Plan (IRP)
- ☐ Assign roles and responsibilities for incident response
- ☐ Conduct regular IRP testing and simulations
- ☐ Log and report incidents per DFARS 7012 requirements
- ☐ Train staff on how to report and escalate incidents

7. Maintenance (MA)

Ensure systems are maintained securely.

- ☐ Approve and track all maintenance activities
- ☐ Control remote maintenance with MFA
- ☐ Sanitize media prior to offsite maintenance
- ☐ Inspect tools for malicious code
- ☐ Document and review maintenance actions

8. Media Protection (MP)

Prevents unauthorized access to data on storage devices.

- ☐ Encrypt CUI on all storage and transmission platforms
- ☐ Restrict use of USBs and external drives
- ☐ Securely erase media before disposal or reuse
- ☐ Track media use and access
- ☐ Label and control portable storage devices

9. Personnel Security (PS)

Reduce risk through personnel screening and oversight.

- ☐ Screen individuals prior to granting access
- ☐ Revoke access upon termination or transfer
- ☐ Ensure personnel sign acceptable use policies
- ☐ Maintain records of access approvals and revocations

10. Physical Protection (PE)

Safeguards facilities and equipment from unauthorized physical access.

- ☐ Restrict access to sensitive equipment areas
- ☐ Log and monitor visitor access
- ☐ Escort visitors in secure spaces
- ☐ Use badge or keycard access control
- ☐ Secure backup media in locked containers
- ☐ Protect alternative workspace locations

11. Risk Assessment (RA)

Identifies and addresses potential cybersecurity risks.

- ☐ Conduct regular risk assessments
- ☐ Identify vulnerabilities through scanning
- ☐ Prioritize risk remediation based on impact
- ☐ Incorporate threat intelligence into assessments

12. Security Assessment (CA)

Monitors and improves your security program.

- ☐ Review and update the System Security Plan (SSP)
- ☐ Maintain and execute a Plan of Action & Milestones (POA&M)
- ☐ Conduct internal security control assessments
- ☐ Monitor the effectiveness of corrective actions

13. System and Communications Protection (SC)

Secures the flow of information across your network.

- ☐ Use encryption for all CUI in transit and at rest
- ☐ Maintain updated firewalls and antivirus tools
- ☐ Segment networks to limit lateral movement
- ☐ Monitor internal and external network traffic
- ☐ Control communications at system boundaries
- ☐ Manage mobile code, VoIP, and remote sessions

14. System and Information Integrity (SI)

Ensures systems and data are monitored for integrity and threats.

- ☐ Deploy malware protection and intrusion detection
- ☐ Keep systems patched and updated
- ☐ Scan files for malicious code
- ☐ Respond to system alerts promptly
- ☐ Monitor for unauthorized use or anomalous activity

Common CMMC Compliance Mistakes

- ✖ Assuming antivirus = compliance
- ✖ Relying solely on your IT guy to “handle it”
- ✖ Not documenting your policies and procedures
- ✖ Forgetting to train users annually
- ✖ Thinking a firewall is enough for CUI
- ✖ Not preparing for DFARS 7012 reporting

Why CMMC Compliance Matters

- ✓ Required for DoD contracts
- ✓ Protects your ability to bid on future work
- ✓ Reduces risk of cyber breaches and insider threats
- ✓ Builds trust with Primes and auditors
- ✓ Failure to comply = loss of revenue and reputation

Your Next Steps

- ☐ Review your checklist results
- ☐ Prioritize your top 3 risk areas
- ☐ Book a **free 15-minute Discovery Call**