CMMC
Audit Preparation Checklist

General Preparation

1 **Review the CMMC Model documentation, including**:
FAR 52.204.21 https://www.acquisition.gov/far/52.204-21
NIST 800-171 Rev. 2 https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final
NIST-172 https://csrc.nist.gov/pubs/sp/800/172/final

2 **Determine the level of compliance** you'll need based on what type of information your company handles and the specific requirements of the contracts you want to pursue with the DoD. Consider the complexity and scope of your work. If in doubt, consult with the DoD or a certified third-party assessor organization (C3PAO).

3 **Conduct a gap analysis** against NIST 800-171 controls.

4 **Develop a remediation plan** to address identified gaps. Your plan should establish timelines and needed resources for remediation efforts.

5 **Implement any necessary changes** to meet CMMC requirements including new administrative controls and new technical controls such as access controls, encryption, continuous monitoring, and identification and multi-factor authentication.

6 **Conduct an internal audit** to ensure you have the right tools, policies, and procedures in place to close all gaps. An MSP can assist in creating and maintaining the necessary documentation, technical configurations, and training records required, making it easier to demonstrate compliance during the official audit.

7 **Engage a** **CMMC Registered Provider Organization** to guide you through the assessment process. An RPO is an organization that has been trained and certified by Cyber-AB and possesses in-depth knowledge of the CMMC framework and its requirements across all levels. An RPO can help you address any remaining issues identified during the pre-assessment.

8 **Prepare a System Security Plan** (SSP) that describes how your organization's information system is secured. Include the specific security controls, policies, procedures, and configurations in place to protect sensitive data.

9 **Create a Plan of Action & Milestones** (POA&M) document outlining the plan for addressing any deficiencies or gaps in your cybersecurity controls that have been identified.

10 **Compile and organize all necessary documentation and evidence** required for the audit. This will ensure everything is in order and readily available, reducing the likelihood of delays or complications during the office audit.

MIS Solutions, Inc.
www.mis-solutions.com
678-745-5109

Level 1 Foundational Checklist

1 Access Control

- Implement unique user IDs
- Limit information access to authorized users
- Ensure the use of strong passwords and update regularly

2 Identification & Authentication

- Require multifactor authentication (MFA for access
- Implement identity verification processes

3 Media Protection

- Protect physical and digital media containing Federal Contract Information (FCI)
- Sanitize media before disposal or reuse

4 Physical Protection

- Restrict physical access to systems handling FCI
- Implement visitor control systems

5 System & Communication Protection

- Secure transmission of FCI using encryption
- Separate systems that process FCI from public-facing systems

6 Incident Response

- Establish an incident response plan
- Train personnel on incident response procedures

7 Maintenance

- Perform regular system maintenance
- Document and manage maintenance activities

8 Security Assessment

- Conduct regular security assessments
- Implement corrective actions for identified vulnerabilities

Level 2 Advanced Checklist

1 Audit & Accountability

- Enable audit logging on systems processing Controlled Unclassified Information (CUI)
- Regularly review audit logs for suspicious activity

2 Risk Management

- Perform a risk assessment specific to CUI
- Implement risk mitigation strategies

3 Access Control

- Implement role-based access controls (RBAC)
- Monitor and log user access to systems

4 Identification & Authentication

- Use strong, unique identifiers for user authentication
- Regularly rotate cryptographic keys

Level 2 requirements continued

Level 2 Advanced Checklist Continued

5

Configuration Management
- Implement secure configuration settings
- Document and control system configurations

6

Incident Response
- Enhance incident response capabilities for CUI
- Conduct regular incident response drills

7

Security Awareness Training
- Provide cybersecurity awareness training tailored to CUI handling
- Regularly update training materials and records

8

Security Assessment
- Conduct third-party assessments and penetration testing
- Address vulnerabilities identified in assessments

9

System & Communication Protection
- Use VPNs for remote access to CUI
- Implement email protections such as anti-phishing tools

10

System & Information Integrity
- Implement endpoint protection solutions
- Regularly update and patch systems

Level 3 Expert Checklist

1

Advanced Access Control
- Implement Just-In-Time access controls
- Utilize least privilege access principles across the organization

2

Enhanced Audit & Accountability
- Implement advanced analytics to monitor user activity
- Automate responses to detected anomalies

3

Advanced Configuration Management
- Automate configuration management with secure baselines
- Continuously monitor for unauthorized changes

4

Continuous Monitoring
- Implement Security Information and Event Management (SIEM) solutions
- Use advanced threat detection and response tools such as EDR and XDR

5

Advanced Incident Response
- Develop threat-hunting capabilities
- Implement automated incident detection and response tools

6

Advanced Risk Management
- Integrate threat intelligence into risk management practices
- Develop and refine a cyber resilience plan

7

Supply Chain Risk Management
- Assess and manage cybersecurity risks in the supply chain
- Implement contractual requirements for suppliers regarding CUI protection

8

Advanced System & Communication Protection
- Implement micro-segmentation for systems processing CUI
- Enhance encryption standards and key management practices