









## Best Practices for CMMC Maintenance Requirement



Achieving CMMC compliance for the Maintenance domain requires implementing best practices. Here are several strategies defense contractors can employ to ensure their systems and applications are maintained properly to protect controlled unclassified information (CUI) and federal contract information (FCI) in compliance with the Cybersecurity Maturity Model Certification (CMMC) framework:

-  **1. Conduct Regular System Audits:** Systematically review and evaluate your technology infrastructure to detect and address any issues related to system maintenance, which could potentially compromise the functionality and security of the systems.
-  **2. Deploy Automated Patch Management:** Install the latest security patches and updates for software and operating systems to ensure all systems remain up-to-date with the latest security enhancements.
-  **3. Document Maintenance Processes:** Document every step and action taken during maintenance, including the date and time of the activity, the individuals involved, the specific tasks performed, and any materials or parts used.
-  **4. Enlist Third-party Assessments:** Utilize certified third-party assessor organizations (C3PAOs) to review maintenance practices to identify areas that might not meet industry standards or could be optimized for better efficiency and reliability.
-  **5. Implement Change Management Procedures:** Clearly define the changes that need to be made to systems, whether they involve updates, modifications, or fixes. Each change should be meticulously documented to create a comprehensive record.
-  **6. Deploy Access Control Measures:** Establish strict protocols and guidelines that determine who is permitted to access various system functionalities and perform specific tasks. Access controls ensure only authorized personnel, like IT administrators or designated maintenance staff, have the ability to carry out maintenance activities on critical systems and infrastructure.
-  **7. Establish Incident Response Planning:** Develop and maintain a comprehensive incident response plan that is specifically designed to address any security incidents related to maintenance activities.
-  **8. Collaborate with Vendors:** Establish clear communication channels and regular check-ins to discuss compliance expectations and progress. Provide vendors with detailed guidelines and resources to help them understand the maintenance criteria defined by CMMC.