Kiteworks

BEST PRACTICES

CMMC Certification Best Practices Checklist

CMMC Certification Best Practices Checklist

CMMC certification requires companies to meet an extensive set of criteria set by the DoD. Below is our list of CMMC certification best practices your organization should embrace on its path to CMMC certification.

☑ **1. Choose the Appropriate CMMC Maturity Level**
There are three levels of CMMC certification: Level 1 (foundational), Level 2 (advanced), and Level 3 (expert); companies must choose the right level to pursue based on the sensitivity of the data they handle. Certification requirements increase in stringency in parallel to the sensitivity of content to be handled and shared.

☑ **2. Perform a CMMC Self-assessment**
Conduct a self-assessment of your cybersecurity profile to gauge your readiness for CMMC certification. This assessment should include a review of your cybersecurity maturity, including your policies and procedures, network security, access control, and incident response capabilities.

☑ **3. Leverage Complementary Cybersecurity Frameworks**
CMMC was developed from existing frameworks and significant overlap is evident. Leveraging existing frameworks and certifications that align with CMMC requirements can make CMMC certification less daunting. Complementary frameworks include the NIST Cybersecurity Framework (NIST CSF), FedRAMP, FISMA, ISO 27001, and NIST Special Publication 171-800.

☑ **4. Build a Plan of Action and Milestones (POA&M)**
A Plan of Action and Milestones (POA&M) outlines your strategy to address its cybersecurity weaknesses and deficiencies. Once you identify the gaps between your current cybersecurity posture and your desired CMMC certification level, prioritize the areas that need to be addressed. Develop a timeline for each task, assign tasks to team members with clear responsibilities, and document all the steps taken. Keep track of progress and update the POA&M as needed.

☑ **5. Develop a System Security Plan (SSP)**

The SSP outlines your organization’s authentication and authorization procedures, information flows, company regulations, staff security obligations, network diagrams, administrative duties, and more. Note: creating and updating the SSP can be a resource-intensive process but it’s a critical component of the certification process. The Defense Department will evaluate your SSP.

☑ **6. Select a CMMC Third Party Assessor Organization (C3PAO)**

A C3PAOs is authorized to conduct CMMC assessments. They provide guidance throughout the compliance process and assess your organization’s compliance with the CMMC framework. When selecting a C3PAO:

- Check the CMMC-AB website for a list of authorized C3PAOs
- Look for a C3PAO with experience in your industry
- Check the C3PAO’s accreditation status
- Ask for references
- Look at their pricing structure

☑ **7. Set a Timeline**

The CMMC certification process can take up to 12 months, with ongoing maintenance and periodic assessments throughout, so plan accordingly. Other variables include your desired level of certification, your organization’s size and current cybersecurity posture. Also keep in mind the C3PAO’s gap analysis can take up to three months.

☑ **8. Allocate Sufficient Resources**

The CMMC certification process can be costly from both a financial and personnel allocation perspective, so companies must budget accordingly. Contractors should plan to incur costs for cybersecurity assessments, remediation, and ongoing maintenance. Keep in mind the following when planning your budget:

- Certification costs can vary depending on the CMMC level you’re pursuing
- C3PAO costs can vary based on their experience and accreditation status
- Certification requires ongoing maintenance, and additional cost