CMMC Compliance Checklist

Sourced and condensed from encryption authority Preveil's guide, here is a comprehensive checklist to help you track your CMMC compliance progress.

1. Determine your CMMC level based on the type of data you handle

- ☐ Assess whether your organization handles Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) to determine the necessary level of CMMC compliance.
- ☐ Review your contracts to identify the level specified by DoD or other government agencies to ensure you are in compliance.

2. Designate a compliance point person

- ☐ Assign a single person within your organization to own the CMMC compliance process and coordinate efforts across various departments to ensure timely implementation of compliance measures, and liaise with external parties if necessary.

3. Identify and limit the scope of CUI within your environment

- ☐ Determine where CUI resides within your organization's systems and networks.
- ☐ Streamline the CUI environment to minimize the number of endpoints and personnel with access, in order to reduce complexity and costs.
- ☐ Restrict the scope of CUI to reduce the attack surface and enhance the effectiveness of your security measures.

4. Restrict access to CUI to critical personnel

- ☐ Limit access to CUI only to individuals who require it for their job responsibilities.
- ☐ Implement robust access controls and authentication mechanisms to prevent unauthorized access to sensitive information.
- ☐ Restrict access to essential personnel and organizations to mitigate the risk of data breaches and unauthorized disclosures.

5. Select compliant technologies for CUI protection

- ☐ Choose technology solutions that meet the stringent security requirements for protecting CUI.
- ☐ Ensure selected technologies incorporate encryption standards such as FIPS 140-2 validation for securing CUI during transmission and storage.
- ☐ Ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP) standards if you're a cloud service provider (CSP) hosting CUI.

6. Retain a CMMC Registered Practitioner (RP), if desirable

- ☐ Consider engaging a CMMC RP to assist in implementing technologies, organizing documentation, and identifying compliance gaps.
- ☐ While optional, hiring a registered provider organization (RPO) can streamline the compliance journey and ensure thorough preparation for assessment.

7. Develop a comprehensive System Security Plan (SSP)

- ☐ Create a detailed System Security Plan (SSP) that outlines your organization's cybersecurity program and how it meets the required controls to serve as a roadmap for assessors, in demonstrating compliance with NIST 800-171 or other relevant standards.
- ☐ Regularly update the SSP to reflect changes in the organization's systems and security posture.

8. Establish a Plan of Action and Milestones (POA&M)

- ☐ Identify controls that are not fully met and develop a Plan of Action and Milestones (POA&M) to address deficiencies.
- ☐ Outline specific actions, timelines, and resources required to remediate non-compliant controls.
- ☐ Regularly review your POA&M, update it, and track progress towards your compliance goals.

9. Conduct a self-assessment against NIST 800-171A

- [ ] Perform a thorough self-assessment against the objectives outlined in NIST 800-171A to gauge compliance readiness, evaluate strengths and weaknesses, and inform of remediation efforts.
- [ ] Assess adherence to all relevant controls and objectives to ensure alignment with the desired CMMC level.

10. Remediate any identified security gaps

- [ ] Address identified security gaps by implementing the necessary measures outlined in the POA&M.
- [ ] Prioritize remediation efforts based on the severity and impact of each security gap.
- [ ] Close any noted security gaps to strengthen overall cybersecurity posture and enhance readiness for assessment.

11. Optionally, seek final review from an RPO or C3PAO

- [ ] Consider engaging an RPO or Certified Third-Party Assessment Organization (C3PAO) for a final review before the formal assessment to ensure readiness and identify any remaining compliance gaps.

12. Schedule a C3PAO assessment for certification

- [ ] Arrange for a C3PAO to conduct the formal assessment for CMMC certification.
- [ ] Complete the assessment and await your results.