RACKTOP

CMMC Preparedness Checklist

The United States Department of Defense Cybersecurity Maturity Model Certification (CMMC) program mandates that all US DoD RFP's comply with CMMC third party certification to protect controlled classified information. Our CMMC Preparation Checklist will help you implement a manageable and cost-effective plan for your organization.

- [ ] 1. Attend informational sessions on what CMMC is and how it will affect your organization.
- [ ] 2. Communicate to your entire workforce what CMMC is, why it is important to your organization and the nation, and how it will affect day to day operations and the long-term success of the business.
- [ ] 3. Document your current Administrative and IT processes:

  The processes around the lifecycle of an employee, contractor, or visitor should be documented, covering how they are onboarded, trained, monitored, and what happens when they leave voluntarily or involuntarily.
- [ ] 4. Assign Executive/Management Ownership to each domain within the CMMC.
- [ ] 5. Establish who is authorized to approve and change processes.
- [ ] 6. Establish who is going to sign off and attest that processes are being followed.
- [ ] 7. Establish a committee within the organization that is responsible for reviewing processes.
- [ ] 8. Setup a review period for each policy. Recommend quarterly reviews for a new initiative.
- [ ] 9. Perform internal audits of compliance with established policies at least twice per review period to ensure the policies are effective and in force. Report findings to executive management assigned in step 4.
- [ ] 10. Establish an Emergency Action Group and Escalation Procedures.