Sg Strike Graph

CMMC Level 2 Compliance Checklist

Step	Description	Key Details
□ 1. Confirm applicability	Verify if CMMC applies to your contracts	• Review contracts for the DFARS 7012 clause, which mandates compliance with NIST SP 800-171 • Subcontractors should confirm compliance obligations with the prime contractor • If you need Level 2 compliance: Confirm whether your contract requires Level 2 certification from a Certified Third-party Assessor Organization (C3PAO), or if you only need to complete and submit a self-assessment
□ 2. Determine scope & set a timeline	Identify parts of your systems needing CMMC controls	• Align the next steps with contractual deadlines • Use the DoD CMMC 2.0 Level 2 scoping guidelines to define your CMMC scope • Consider segmenting relevant systems to save money, time, and effort
□ 3. Develop a System Security Plan (SSP)	Create a plan for managing required controls	• Use industry-standard SSP templates to document CMMC requirements • Include details about your existing cyber security environment, the status of each control (implemented, planned, or not applicable), and plans to meet any unmet requirements • Ensure your SSP also contains a clause that outlines how often you will update it
□ 4. Conduct a self-assessment	Evaluate your current compliance status	• Perform an internal review of your systems against CMMC 2.0 Level 2 requirements • Use the DoD’s SPRS system to calculate a Supplier Performance Risk System (SPRS) Score to see whether you are fully compliant (score of 110) • Track areas where you did not fully meet the security control requirements
□ 5. Draft a Plan of Action and Milestones (POAM)	Address weaknesses with remediation plans	• Create a detailed POAM to document gaps in your self-assessment and plan to remediate them • Include details like a full description of each deficiency, actionable steps to address the gap, deadlines, and responsibilities • Implement your POAM and recalculate your SPRS score after • Develop plans for non-compliant areas • Prioritize critical vulnerabilities that impact your SPRS score
□ 6. Engage a C3PAO OR submit a self-assessment	Hire a Certified Third-Party Assessment Organization (C3PAO) for an external audit, or formally complete a self-assessment and submit your SPRS score	• For a C3PAO assessment: Select a C3PAO from the official Cyber-AB Marketplace. • Be ready for a thorough audit where the C3PAO will test and verify your compliance with the 110 NIST SP 800-171 controls • For a self-assessment: Use the DoD’s CMMC Level 2 Assessment Guide to conduct a detailed internal review of your system against the CMMC Level 2 SPRS system to calculate and submit your SPRS score.
□ 7. Maintain compliance	Keep your certification current	• Conduct annual self-assessments to monitor and address any vulnerabilities or changes • Submit your annual affirmation annually, as required by CMMC guidelines • Plan for re-certification every three years, as required by CMMC guidelines • Stay informed about updates to NIST SP 800-171 and CMMC policies