C3 INTEGRATED SOLUTIONS

Five Keys to CMMC Level 2 Success

Achieving CMMC Level 2 compliance takes more than checking boxes. These five keys show how to build a secure environment, sustain compliance, and achieve assessment success – with C3 supporting you every step of the way.

1 Build a Strategy

- Review contracts (e.g., DFARS 7012) and business plans.
- Identify if you handle FCI or CUI.
- Choose your boundary approach:
  - Enclave: smaller scope, lower cost, but more complexity.
  - All-in: unified security, higher upfront cost.
  - Define systems, boundaries, and data flows.

2 Deploy Technical Solutions

- Use FedRAMP-equivalent systems when required.
- Align asset configs with NIST SP 800-171A Rev 2.

3 Manage Environments

- Continuously patch, update, and manage changes.
- Ensure policies and procedures are mapped to NIST 800-171A Rev 2.
- Implement change management practices

4 Conduct Security Monitoring

- Implement real-time monitoring across systems.
- Conduct vulnerability scans, threat hunting, and ongoing monitoring.
- Track activity through logging, auditing, and alerts.
- Build incident response plans and run tabletop exercises.

5 Manage Compliance

- Build and maintain policies, SSP, diagrams, and data flows.
- Update artifacts and POA&Ms regularly.
- Treat compliance as a continuous cycle, not a one-time event.

Key Takeaway:

The C3 Suite supports every step – ensuring a secure environment and positioning you for CMMC assessment success.

Contact us to get started.