(650) 575-9435

CMMC LEVEL II COMPLIANCE BUDGET & REQUIREMENT WHITEPAPER

As the federal government continues to advance it's CMMC Compliance program Defense Contractors can expect to be required in the next 6 months (in some contract offerings sooner) to have Level II C3PAO certification with regards to their Cybersecurity and protection of United Stated Controlled Unclassified Information (CUI)

The following is an overview of what you can expect if you are looking to move towards Level II Certification. At this time Level III will likely only be required for Defense Contractors handling highly sensitive controlled information. The majority however will require at least Level II Certification and that certification will need to be completed by a Certified Third Party Assessment Organization (C3PAO). Presently 65 in the nation.

Frisco IT Services is a full-service IT Managed Services and Cybersecurity company with the resources to get you audit ready and support you during the audit. We have partnered with A-Lign one of the largest C3PAO firms in the nation to provide you the preparation, audit support, and post support compliance to ensure you can confidently bid on contracts requiring CMMC Compliance.

Here is what you should expect and plan for if you are planning to complete the CMMC Level II Certification process:

1) Discontinuation of Self-Assessments: Self-Assessments by the contract awardee will likely no longer be admissible except for contracts requiring a Level I compliance. (17 controls) – See Appendix I
2) Requirement for Level II Compliance to be certified by a C3PAO assessors. C3PAO assessors are companies/individuals who have undergone additional training and certification by The Cyber AB, the official, Non-Profit accreditation and certification body that supports the US Department of Defense. There are presently 100 C3PAO providers. Level II consists of 110 controls and a significant amount of documentation and artifacts before you should consider undergoing a Level II

C3PAO audit. In most cases, you will want to bring-on additional support from an outside consultant with CMMC Compliance experience. The process to prepare for a Level II CMMC C3PAO Audit can take upwards of 700 plus man hours just to prepare and many C3PAO bodies will not even consider you for an audit without demonstrating you are well ahead in meeting all 110 controls.

Approximate Time & Cost For Level II Certification – (Budgetary Overview)

Task/Requirement	Estimated Man Hours	Estimated Cost
Documentation of compliance with NIST Controls for Level II (110)	300 man hours	Internal: Your resource cost External: Avg: $110 an hour
Implement Secure Enclave	20 (PreVeil) 400 (MS GCC High)	PreVeil: $5,000 (3 users, $550 each additional user, annual) (All individuals accessing CUI must have a license) MS GCC High: $1200 each user, annual plus $15-25K implementation and configuration
External/Internal Pentest	40 hours	$10,000-$25,000
SIEM Solution (Security Information & Event Management) – manages/consolidates logs, scans networks for vulnerabilities, proactively monitors using AI, early detection, and alerting. (Often managed by a third party Secure Operations Center (Soc) but can be managed internally. Some solutions include: MS Sentinel, Splunk, etc.)	5 hours (implementation)	$480 per user, annually $1000 implementation (1x)
EDR/MDR (Endpoint Detection and Response, Antivirus, Anti-Malware, Advanced Threat Detection, and Managed Detection & Response, 3rd party threat monitoring solution (should be on all	5 hours (implementation) plus installation on each device. Continuous monitoring of EDR/MDR/SIEM should be performed by a third-party SOC. This can be a full-time job for a professional,	$300 per user, annually $1000-2000 implementation (1x)

company endpoints operating on a corporate network, must be on all devices managing CUI. Implementing an EDR/MDR/SIEM that is continuously monitored by a third-party SOC is recommended.	certified, Cyber analyst if you attempt to meet this requirement internally.	
Pre-Assessment (non-C3PAO) review SSP/Documentation, conduct pre-assessment compliance check to prepare for third party audit (C3PAO)	100 man hours	Internal: Your resource cost (not recommended) External: $110 per hour average
C3PAO Scoping	20 man hours	External: $220 per hour
C3PAO Level II Assessment	80 man hours	External: $40,000-$80,000 and rising as demand increases and resources decrease

SUMMARIZED COST

Software/Licensing:	First Year: Annual Recurring:	$2480 $1330
Annual Pentest:	Annual Minimum	$10,000-$25,000
Professional Services	Quarterly/Annual: to review and assess ongoing compliance.	$110 per hour average, budget 80 hours – quarter - $8,800
Pre-Assessment	Not required but recommended Every two-three years	$110 per hour Average, budget 100 hours - $11,000
C3PAO Audit	Initial Audit Triennial Audits	$40,000-$80,000 $40,000-$80,000
PROJECTED FIRST TIME TOTAL:		**$72,280-$130,000**

These costs are estimated. Frisco IT Can help you minimize the non C3PAO services costs with our annual CIO On Demand/Managed Services plan. Starting at $5900 per month these plans offer a full time Helpdesk, System Engineer, Cybersecurity Analyst, and Virtual CIO and all non

C3PAO related services and hours are INCLUDED! Plus all the above, unlimited helpdesk support, 1-2 monthly office visits, professional IT consulting, IT Project/Budget management, Facilities/Security Management, and you own IT SME on demand! FOR LESS COST THAN A SINGLE HELPDESK ANALYST!

Call (650) 575-9435 if you are ready to begin your CMMC Compliance Certification or need a full time IT Team for the cost of one FTE!

www.friscoitservices.us

APPENDIX 1 - CMMC Level 1 Controls Overview

CMMC (Cybersecurity Maturity Model Certification) Level 1 compliance establishes basic cyber hygiene practices for organizations handling Federal Contract Information (FCI).

CMMC Level 1 has a total of 17 practices (commonly referred to as controls).

Summary of CMMC Level 1 Controls

Level 1 is mapped directly to the **17 controls in FAR 52.204-21**, which are considered foundational. These practices cover:

- **Access Control** – Limit access to authorized users/devices.
- **Identification and Authentication** – Ensure users/devices are properly identified before access.
- **Media Protection** – Handle and dispose of media containing FCI appropriately.
- **Physical Protection** – Limit physical access to systems.
- **System and Communication Protection** – Control network communications.
- **System and Information Integrity** – Protect against malicious code and promptly repair flaws.

The 17 Specific Practices (Controls)

1. **AC.1.001** – Limit information system access to authorized users, processes acting on behalf of authorized users, and devices.
2. **AC.1.002** – Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
3. **AC.1.003** – Verify and control/limit connections to and use of external information systems.
4. **AC.1.004** – Control information posted or processed on publicly accessible systems.
5. **IA.1.076** – Identify information system users, processes acting on behalf of users, or devices.
6. **IA.1.077** – Authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to system access.
7. **MP.1.118** – Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
8. **PE.1.131** – Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
9. **PE.1.132** – Escort visitors and monitor visitor activity.
10. **PE.1.133** – Maintain audit logs of physical access.

11. **PE.1.134** – Control and manage physical access devices.
12. **SC.1.175** – Monitor, control, and protect organizational communications (e.g., information transmitted or received over networks) at the external boundaries and key internal boundaries of information systems.
13. **SC.1.176** – Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
14. **SI.1.210** – Identify, report, and correct information and information system flaws in a timely manner.
15. **SI.1.211** – Provide protection from malicious code at appropriate locations within organizational information systems.
16. **SI.1.212** – Update malicious code protection mechanisms when new releases are available.
17. **SI.1.213** – Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Key Points to Remember

- **Documentation:** Level 1 does not require formal process documentation or process maturity. The focus is simply on performing these practices.
- **Scope:** These controls apply to all systems and environments processing FCI.
- **Assessment:** Assessments are conducted by a C3PAO (CMMC Third-Party Assessment Organization) to confirm you are performing all 17 practices. For Level I, self-assessments may be allowed.

APPENDIX 2 - CMMC Level 2 – What You Must Do

This level is a **big step up** from Level 1. Level 2 is all about demonstrating **good cybersecurity practices and protecting Controlled Unclassified Information (CUI)**.

---

1. Implement All 110 Controls

CMMC Level 2 **directly aligns with the 110 security requirements in NIST SP 800-171**.
These controls fall into 14 families:

- **Access Control** – E.g., limit who can access CUI and how.
- **Awareness and Training** – Train users on security risks and responsibilities.
- **Audit and Accountability** – Generate and review audit logs.
- **Configuration Management** – Maintain secure configurations.
- **Identification and Authentication** – Use multifactor authentication and strong account management.
- **Incident Response** – Prepare, detect, respond, and recover from incidents.
- **Maintenance** – Control maintenance activities, including remote maintenance.
- **Media Protection** – Protect and sanitize media containing CUI.
- **Personnel Security** – Screen and offboard personnel.
- **Physical Protection** – Limit physical access.
- **Risk Assessment** – Perform vulnerability scanning and risk analysis.
- **Security Assessment** – Develop and maintain a system security plan and conduct self-assessments.
- **System and Communications Protection** – Protect data in transit and at rest.
- **System and Information Integrity** – Monitor systems, patch vulnerabilities, and prevent malware.

If you have CUI, you must **implement and document all 110 controls**.

---

2. Develop Required Documentation

Unlike Level 1, **Level 2 requires formal documentation**:

- **System Security Plan (SSP)**
  - Describes how you implement each control.
  - Must be up to date and complete.
- **Plans of Action and Milestones (POA&M)**
  - Describes any gaps and how you plan to fix them.
- **Policies and Procedures**

    - Written policies to show your organization's expectations and practices.
- **Incident Response Plan**
    - Formal process for detecting, responding, and recovering from incidents.

---

3. Pass an Assessment by a Certified Assessor

- For contracts involving **CUI**, **third-party assessments** are required.
    - These are conducted by a **Certified Third-Party Assessment Organization (C3PAO)** accredited by **The Cyber AB**.
- The assessor will:
    - Evaluate whether each of the 110 controls is implemented and effective.
    - Review your documentation.
    - Interview staff and examine evidence.
- If you pass, you receive a **Level 2 CMMC Certificate** valid for 3 years.

---

4. Maintain Ongoing Compliance

- **CMMC is not a one-time effort.** You must:
    - Keep your SSP and POA&M up to date.
    - Continuously monitor and improve security.
    - Prepare for reassessment every 3 years (or sooner if required).

Quick Recap

To achieve Level 2 CMMC Compliance, you must:

1. Implement all 110 NIST SP 800-171 controls.
2. Maintain complete and current documentation.
3. Undergo and pass a C3PAO assessment.
4. Continuously monitor and update your security program.

CMMC Level 2 – The 110 Controls (NIST SP 800-171)

---

1. Access Control (AC) – 22 Controls

1. AC.1.001 – Limit system access to authorized users.
2. AC.1.002 – Limit system access to permitted transactions/functions.
3. AC.1.003 – Verify and control/limit connections to external systems.
4. AC.1.004 – Control information posted on publicly accessible systems.
5. AC.2.005 – Use least privilege.
6. AC.2.006 – Limit use of non-organizational systems.
7. AC.2.007 – Employ session lock.
8. AC.2.008 – Terminate sessions after inactivity.
9. AC.2.009 – Control remote access.
10. AC.2.010 – Authorize remote execution of privileged commands.
11. AC.2.011 – Authorize wireless access prior to connection.
12. AC.2.012 – Protect wireless access using authentication and encryption.
13. AC.3.013 – Monitor/control remote access methods.
14. AC.3.014 – Route remote sessions through managed network.
15. AC.3.015 – Authorize and monitor remote access to privileged accounts.
16. AC.3.016 – Limit unsuccessful login attempts.
17. AC.3.017 – Employ cryptographic session protections.
18. AC.3.018 – Prevent reuse of identifiers.
19. AC.3.019 – Disable identifiers after inactivity.
20. AC.3.020 – Use replay-resistant authentication mechanisms.
21. AC.3.021 – Prevent access by terminated or transferred users.
22. AC.3.022 – Use mobile device controls.

---

2. Awareness and Training (AT) – 3 Controls

23. AT.2.056 – Ensure personnel are aware of security risks.
24. AT.2.057 – Provide role-based security training.
25. AT.3.058 – Provide insider threat awareness training.

---

3. Audit and Accountability (AU) – 9 Controls

26. AU.2.041 – Create and retain audit records.
27. AU.2.042 – Ensure audit records contain required content.
28. AU.2.043 – Review and update logged events.

29. AU.3.044 – Alert on audit processing failures.
30. AU.3.045 – Correlate audit record review and analysis.
31. AU.3.046 – Provide audit reduction and reporting capability.
32. AU.3.047 – Protect audit information and tools.
33. AU.3.048 – Limit audit management to authorized users.
34. AU.3.049 – Review/analyze audit logs weekly.

---

4. Configuration Management (CM) – 9 Controls

35. CM.2.061 – Establish configuration baselines.
36. CM.2.062 – Enforce security configuration settings.
37. CM.2.063 – Track/review/approve/disapprove/log changes.
38. CM.2.064 – Analyze security impact of changes.
39. CM.2.065 – Define/approve/limit device connections.
40. CM.3.066 – Employ configuration management for security.
41. CM.3.067 – Restrict nonessential functions/services/ports.
42. CM.3.068 – Apply deny-all, permit-by-exception policy.
43. CM.3.069 – Control user-installed software.

---

5. Identification and Authentication (IA) – 11 Controls

44. IA.1.076 – Identify users/devices.
45. IA.1.077 – Authenticate identities.
46. IA.2.078 – Enforce multifactor authentication.
47. IA.2.079 – Uniquely identify/authenticate users.
48. IA.3.080 – Use replay-resistant authentication.
49. IA.3.081 – Prevent reuse of passwords.
50. IA.3.082 – Protect authenticators during transmission/storage.
51. IA.3.083 – Obscure feedback of authentication info.
52. IA.3.084 – Use device authentication.
53. IA.3.085 – Enforce account management policies.
54. IA.3.086 – Use cryptographic authentication.

---

6. Incident Response (IR) – 7 Controls

55. IR.2.092 – Establish incident response capability.
56. IR.2.093 – Detect/report incidents.
57. IR.2.094 – Analyze incidents.

58. IR.2.095 – Contain incidents.
59. IR.2.096 – Eradicate incidents.
60. IR.2.097 – Recover from incidents.
61. IR.2.098 – Test incident response capability.

---

7. Maintenance (MA) – 6 Controls

62. MA.2.111 – Perform system maintenance.
63. MA.2.112 – Approve/monitor maintenance personnel.
64. MA.2.113 – Control remote maintenance.
65. MA.3.114 – Supervise maintenance activities.
66. MA.3.115 – Sanitize equipment before maintenance.
67. MA.3.116 – Check media for malicious code after maintenance.

---

8. Media Protection (MP) – 9 Controls

68. MP.1.118 – Sanitize/destroy media before disposal.
69. MP.2.119 – Protect media during transport.
70. MP.2.120 – Limit access to media.
71. MP.3.121 – Control access to CUI on media.
72. MP.3.122 – Encrypt CUI during transport.
73. MP.3.123 – Restrict use of removable media.
74. MP.3.124 – Prohibit non-org media on systems.
75. MP.3.125 – Sanitize media before reuse.
76. MP.3.126 – Protect CUI stored outside controlled areas.

---

9. Personnel Security (PS) – 2 Controls

77. PS.2.127 – Screen individuals prior to access.
78. PS.2.128 – Ensure access termination or transfer procedures.

---

10. Physical Protection (PE) – 6 Controls

79. PE.1.131 – Limit physical access.
80. PE.1.132 – Escort/monitor visitors.
81. PE.1.133 – Maintain physical access logs.

82. PE.1.134 – Manage physical access devices.
83. PE.3.135 – Protect/monitor physical facility and infrastructure.
84. PE.3.136 – Enforce physical access authorizations.

---

11. Risk Assessment (RA) – 3 Controls

85. RA.3.144 – Periodically assess risk.
86. RA.3.145 – Scan for vulnerabilities.
87. RA.3.146 – Remediate vulnerabilities.

---

12. Security Assessment (CA) – 4 Controls

88. CA.2.157 – Develop/update SSP.
89. CA.2.158 – Develop/implement security assessment plans.
90. CA.3.161 – Monitor security controls effectiveness.
91. CA.3.162 – Remediate deficiencies in controls.

---

13. System and Communications Protection (SC) – 16 Controls

92. SC.1.175 – Monitor/control communications.
93. SC.1.176 – Separate publicly accessible systems.
94. SC.2.178 – Protect CUI at rest.
95. SC.3.177 – Employ cryptographic protections.
96. SC.3.179 – Prevent split tunneling.
97. SC.3.180 – Terminate network connections after inactivity.
98. SC.3.181 – Deny by default, allow by exception.
99. SC.3.182 – Protect integrity of information at rest.
100. SC.3.183 – Use FIPS-validated cryptography.
101. SC.3.184 – Control communications at boundaries.
102. SC.3.185 – Use cryptographic mechanisms for remote access integrity.
103. SC.3.186 – Separate user/system management functionality.
104. SC.3.187 – Prevent unauthorized exfiltration.
105. SC.3.188 – Authenticate communications sessions.
106. SC.3.189 – Use DNS protections.
107. SC.3.190 – Segregate network segments.

---

14. System and Information Integrity (SI) – 7 Controls

108. SI.1.210 – Identify/report/correct system flaws.
109. SI.1.211 – Protect against malicious code.
110. SI.1.212 – Update malicious code protections.
111. SI.1.213 – Perform periodic and real-time scans.
112. SI.2.214 – Monitor security alerts/advisories.
113. SI.3.217 – Implement advanced threat protection.
114. SI.3.218 – Ensure systems are free of known vulnerabilities.