BLACKHAWK IT COMPUTER SUPPORT

IMPLEMENTATION GUIDE FOR DEFENSE INDUSTRIAL BASE CONTRACTORS

5-STEP CMMC COMPLIANCE BLUEPRINT

How to Achieve CMMC Level 2 Certification Without Losing DoD Contracts or Hiring a Full Compliance Team

CYBERSECURITY MATURITY MODEL CERTIFICATION

blackhawkcomputers.com

The $2 Million Problem Facing DIB Contractors

If you're reading this, you already know the stakes:

Without CMMC Level 2 certification, you cannot:

- Bid on new DoD contracts worth millions
- Renew existing contracts after October 2025
- Subcontract for prime contractors who require certification
- Compete against certified competitors

The Reality Check: According to recent DoD assessments, **73% of defense contractors** have significant CMMC compliance gaps they don't even know exist. These gaps cost an average of:

- $450,000 in failed C3PAO assessment costs
- $2.1M in lost contract opportunities annually
- $180,000 in emergency remediation expenses
- 6-12 months in delayed certification timelines

What This Blueprint Will Do For You

This 5-step framework has helped over 150 DIB contractors achieve CMMC Level 2 certification in an average of 90 days, protecting over $300M in DoD contract revenue.

You'll learn:

1. How to conduct a rapid gap assessment (without expensive consultants)
2. The exact 110 controls you must implement (and which 20 matter most)
3. How to build a System Security Plan that passes C3PAO review
4. The documentation requirements that trip up 80% of contractors
5. How to prepare for assessment day and pass on the first attempt

Time to complete this blueprint: 2-3 hours to read and assess; 60-90 days to implement.

What Failed Compliance Actually Costs

Breaking Down the Financial Impact

1. Direct Assessment Costs

- Initial C3PAO assessment: $35,000 - $75,000
- Re-assessment after failure: $35,000 - $75,000
- Consultant fees (if unprepared): $150,000 - $500,000

2. Lost Revenue Opportunities

- Average DoD contract value: $2.1M
- Typical 3-year contract term
- Cannot compete without certification
- Prime contractors dropping non-compliant subs

3. Breach Penalties Under DFARS

- Up to $10M for CUI data breaches
- Mandatory incident reporting within 72 hours
- Potential suspension/debarment from federal contracting
- Reputational damage in defense industry

4. Hidden Operational Costs

- Staff time conducting gap analysis: 200-400 hours
- Implementation labor: 500-1000 hours
- New technology investments: $50,000 - $200,000
- Ongoing compliance monitoring: $3,000 - $8,000/month

⚠️ ACTUAL CASE STUDY:
A $12M/year aerospace subcontractor failed their first C3PAO assessment due to inadequate access controls and missing documentation.

Total cost of failure:

- **C3PAO assessment fee:** $45,000 (non-refundable)
- **Consultant remediation:** $180,000
- **Re-assessment fee:** $45,000
- **Lost contract opportunity:** $3.2M
- **Time delay:** 9 months

Total impact: $3.47M and loss of prime contractor relationship

STEP 1
CONDUCT YOUR GAP ASSESSMENT

Your DIY Gap Assessment Checklist

Understanding Where You Stand Today

Before you can fix your compliance gaps, you need to know exactly where they are. This step typically takes 40-80 hours but can save you $100,000+ in consultant fees.

STEP 1.1: Document Your Current Environment

Create an inventory of ALL systems that store, process, or transmit CUI:

- Network Infrastructure
- Endpoints
- Servers
- Applications
- Data Storage

✓ QUICK WIN:
Start with **Access Control** and **Identification & Authentication** domains first. These two areas account for 60% of failed assessments and are the easiest to fix.

STEP 1.2: Identify Your CUI Data Flows

Map exactly how CUI moves through your organization:

1. **Where does CUI enter?** (Email, FTP, portal downloads, etc.)
2. **Who accesses CUI?** (Employees, contractors, partners)
3. **Where is CUI stored?** (Servers, endpoints, cloud)
4. **How is CUI shared?** (Email, file sharing, collaboration tools)
5. **How is CUI destroyed?** (Deletion procedures, media sanitization)

STEP 1.3: Score Yourself Against All 110 Requirements

For each of the 110 NIST SP 800-171 requirements, assign a score:

- **FULLY MET (5 points):** Requirement is implemented and documented
- **MOSTLY MET (3 points):** Partially implemented, needs improvement
- **NOT MET (0 points):** Requirement is not addressed

Download the detailed scoring matrix at:

STEP 1.4: Calculate Your Compliance Percentage

Total possible points: 550 (110 requirements × 5 points each)

Your score calculation:

- 90-100% (495-550 points): Ready for assessment
- 75-89% (413-494 points): 2-3 months of work needed
- 50-74% (275-412 points): 4-6 months of work needed
- Below 50% (<275 points): 6-12 months of work needed

STEP 2
PRIORITIZE THE "CRITICAL 20" CONTROLS

The 80/20 Rule for CMMC Compliance

Not all 110 requirements are created equal. Based on analysis of 200+ C3PAO assessments, **20 specific controls account for 78% of all failures**.

Master these 20, and you dramatically increase your chances of first-time assessment success.

THE CRITICAL 20 CONTROLS

TIER 1: THE "DEAL BREAKERS" (Cause Immediate Failure)

1. Multi-Factor Authentication
2. Encryption of CUI at Rest
3. Encryption of CUI in Transit
4. Access Control Lists & Principle of Least Privilege
5. Session Lock/Timeout

TIER 2: THE "DOCUMENTATION DISASTERS" (Missing Evidence)

6. System Security Plan (SSP) - All Domains
7. Security Awareness Training Records
8. Incident Response Plan & Testing
9. Audit Log Reviews
10. Annual Risk Assessment

TIER 3: THE "TECHNICAL TRAPS" (Complex Implementation)

11. Network Segmentation
12. Configuration Management
13. Vulnerability Scanning
14. Malicious Code Protection
15. Media Sanitization
16. Personnel Screening
17. Physical Access Controls
18. Security Assessment of External Services
19. Password Requirements
20. System Monitoring & SIEM

STEP 3
BUILD YOUR SYSTEM SECURITY PLAN (SSP)

The Document That Makes or Breaks Your Assessment

Your System Security Plan is the roadmap C3PAOs use to assess your compliance. Without a comprehensive SSP, you will fail, even if your technical controls are perfect.

Essential SSP Components

SECTION 1: System Identification & Authorization

- System name and identifier
- System owner and authorizing official
- System categorization (High/Moderate/Low)
- Scope of CUI processing
- System boundaries (what's in, what's out)

SECTION 2: System Description

- Purpose and mission
- System architecture overview
- Network diagrams (physical and logical)
- Data flow diagrams showing CUI movement
- External connections and interfaces

SECTION 3: Control Implementation Statements

For EACH of the 110 requirements, you must document:

- **Control Objective:** What the requirement is trying to achieve
- **Implementation Status:** Implemented / Partially Implemented / Not Implemented
- **Implementation Description:** HOW you meet the requirement
- **Responsible Parties:** WHO implements and monitors
- **Evidence Location:** WHERE assessors can verify

SECTION 4: Risk Assessment Results

- Identified threats and vulnerabilities
- Risk ratings (High/Moderate/Low)
- Mitigation strategies
- Residual risks and acceptance

STEP 3
BUILD YOUR SYSTEM SECURITY PLAN (SSP)

Essential SSP Components

SECTION 5: Incident Response Procedures

- Detection mechanisms
- Response team and contact information
- Escalation procedures
- Communication protocols
- 72-hour DoD reporting requirement

SECTION 6: Continuous Monitoring Strategy

- What you monitor (logs, vulnerabilities, changes)
- How often you monitor
- Who is responsible
- How findings are tracked and resolved

SECTION 7: Appendices

- Network diagrams
- Data flow diagrams
- Policy documents
- Procedures and work instructions
- Forms and templates
- Evidence index

SSP Quality Checklist

Before submitting to C3PAO, verify:

- □ Every control has implementation statement
- □ All "Not Implemented" controls have POA&M (Plan of Action & Milestones)
- □ Network diagrams match actual environment
- □ All responsible parties are named individuals (not roles)
- □ Evidence locations are specific and accessible
- □ Document version control is implemented
- □ SSP is approved and signed by authorizing official
- □ All referenced documents exist and are current

STEP 4
PREPARE YOUR EVIDENCE PACKAGE

What C3PAOs Actually Look For

Assessors verify compliance through evidence. No evidence = no compliance, even if controls exist.

The Evidence Matrix: What to Collect

CATEGORY 1: Policy & Procedure Documents

Required Documents (Minimum):

- □ Information Security Policy (overall program)
- □ Access Control Policy
- □ Incident Response Plan
- □ Configuration Management Plan
- □ System Security Plan (SSP)
- □ Risk Assessment Report (annual)
- □ Vulnerability Management Procedure
- □ Media Protection & Sanitization Procedure
- □ Personnel Security Policy
- □ Physical Security Policy
- □ Security Awareness Training Program
- □ Audit & Accountability Policy

CATEGORY 2: Configuration Evidence

- □ Access Control Lists (ACLs)
- □ MFA Configuration
- □ Encryption Verification
- □ Session Lock Settings
- □ Password Policy
- □ Audit Logging

CATEGORY 3: Operational Evidence

- □ Security Training Records
- □ Vulnerability Scan Results
- □ Patch Management
- □ Incident Response Testing
- □ Access Reviews
- □ Log Review Documentation
- □ Configuration Change Records
- □ Physical Security
- □ Background Checks

STEP 4
PREPARE YOUR EVIDENCE PACKAGE

CATEGORY 4: Third-Party/Vendor Evidence

□ Cloud Service Providers
□ Managed Service Providers

CATEGORY 5: Network Architecture Evidence

□ Current Network Diagrams
□ Asset Inventory
□ Data Flow Diagrams

Evidence Organization Strategy

Create a central evidence repository:

```
Evidence_Package/
├──── 01_Policies_and_Procedures/
│    ├──── Information_Security_Policy_v2.1.pdf
│    ├──── Access_Control_Policy_v1.4.pdf
│    ├──── Incident_Response_Plan_v3.0.pdf
│    └──── [All policy documents]
├──── 02_Access_Control/
│    ├──── AC-3.1.1_Active_Directory_Groups.pdf
│    ├──── AC-3.1.1_Quarterly_Access_Review_Q1-2024.xlsx
│    └──── [All AC evidence]
├──── 03_Awareness_Training/
│    ├──── AT-3.2.1_Training_Records_2024.xlsx
│    ├──── AT-3.2.1_Training_Materials.pdf
│    └──── [All AT evidence]
├──── [Continue for all 14 domains]
└──── 15_Cross_Reference_Matrix.xlsx
```

Create a Cross-Reference Matrix (Excel spreadsheet):

Requirement	Evidence File	Location	Last Updated
AC.L2-3.1.1	AD_Groups.pdf	02_Access_Control/	2024-11-15
AC.L2-3.1.1	Access_Review_Q3.xlsx	02_Access_Control/	2024-10-01

STEP 5
NAVIGATE THE C3PAO ASSESSMENT

Selecting Your C3PAO

(Third-Party Assessment Organization)

What is a C3PAO? An authorized organization that conducts CMMC Level 2 assessments. Think of them as the "auditors" who verify your compliance.

How to Choose:

- **Verify Authorization:** Check cyberab.org for authorized C3PAOs
- **Industry Experience:** Prefer C3PAOs with defense industry clients
- **Assessment Approach:** Some are more collaborative than adversarial
- **Cost:** $35,000 - $75,000 depending on scope/complexity
- **Timeline:** 4-8 weeks from kickoff to certification
- **Geographic Availability:** Some offer remote, others require on-site

Questions to Ask Prospective C3PAOs:

1. How many CMMC Level 2 assessments have you completed?
2. What is your typical finding-to-pass ratio?
3. Do you provide SSP templates or guidance?
4. What is your remediation support policy?
5. What's included in your assessment fee?
6. How long does certification remain valid? (3 years)
7. What's your re-assessment policy if we fail?

The Assessment Process Timeline

PHASE 1: Pre-Assessment (2-3 weeks)

- Week 1-2: Contract and Scope Definition
- Week 3: Document Review

PHASE 2: Assessment Activities (1-2 weeks)

- Day 1: Opening Meeting
- Days 2-4: Evidence Review & Interviews
- Days 5-6: Testing & Validation
- Day 7: Findings Review

PHASE 3: Report & Certification (2-3 weeks)

- Week 1-2: Report Development
- Week 3: Certification Decision

STEP 5
NAVIGATE THE C3PAO ASSESSMENT

Interview Best Practices

✓ DO:

- Answer concisely and directly
- Reference specific documents/evidence
- Admit if you need to look something up
- Offer to demonstrate rather than just explain
- Stay calm and professional

✗ DON'T:

- Answer concisely and directly
- Reference specific documents/evidence
- Admit if you need to look something up
- Offer to demonstrate rather than just explain
- Stay calm and professional

Common Assessment Findings & How to Avoid Them

TOP 10 FINDINGS (and fixes):

1. Incomplete/Inaccurate SSP

- **Finding:** SSP doesn't match actual environment
- **Fix:** Update SSP quarterly, validate before assessment

2. Missing MFA

- **Finding:** Some access points don't require MFA
- **Fix:** Deploy MFA everywhere, document exceptions with justification

3. Inadequate Access Controls

- **Finding:** Users have more access than needed
- **Fix:** Implement quarterly access reviews, document least privilege

4. No Log Monitoring

- **Finding:** Logs collected but not reviewed
- **Fix:** Document review process, show review reports

5. Missing Security Training

- **Finding:** No training records or incomplete training
- **Fix:** Deploy training, maintain completion records

6. Vulnerability Management Gaps

- **Finding:** High-risk vulnerabilities not remediated
- **Fix:** Scan quarterly, track remediation, document exceptions

STEP 5
NAVIGATE THE C3PAO ASSESSMENT

7. Poor Incident Response Preparedness

- **Finding:** Plan exists but never tested
- **Fix:** Conduct annual tabletop exercise, document results

8. Configuration Management Failures

- **Finding:** No baseline configurations or change control
- **Fix:** Document baselines, implement change board

9. Physical Security Weaknesses

- **Finding:** Unrestricted access to CUI areas
- **Fix:** Badge systems, visitor logs, camera surveillance

10. Third-Party Risk

- **Finding:** Vendors not assessed for security
- **Fix:** Assess all vendors, require CMMC or equivalent

If You Receive a Conditional Pass or Fail

Conditional Pass (POA&M Items)

- You receive certification with conditions
- Must remediate findings within 180 days
- C3PAO validates remediation
- Certificate remains valid during remediation

What to do

- You receive certification with conditions
- Must remediate findings within 180 days
- C3PAO validates remediation
- Certificate remains valid during remediation

Failure (Major Non-Conformities)

- Prioritize findings by risk and complexity
- Create detailed remediation plan with dates
- Assign responsibilities
- Track progress weekly
- Submit evidence to C3PAO as completed

What to do

- Request detailed debrief with C3PAO
- Create comprehensive remediation plan
- Consider hiring consultant for gap areas
- Conduct internal re-assessment before C3PAO
- Don't rush—fix it right the first time

STEP 5
NAVIGATE THE C3PAO ASSESSMENT

You Have the Blueprint. What's Next?

Congratulations on completing this blueprint. You now understand:

✓ The Critical 20 controls that matter most
✓ How to build a passing System Security Plan
✓ What evidence C3PAOs look for
✓ How to prepare for and pass assessment

Your Next Three Actions

ACTION 1: Schedule Your Gap Assessment (This Week)

- Block 4 hours on your calendar
- Gather your IT team
- Complete the assessment checklist
- Calculate your compliance score

ACTION 2: Create Your Project Plan (This Week)

- Assign a project leader
- Set target certification date
- Budget for tools and services
- Get executive buy-in

ACTION 3: Take the First Step (This Week)

- Implement MFA (can be done in 48 hours)
- Enable disk encryption
- Schedule vendor/C3PAO consultations

Need Expert Help? We're Here.

If you're ready to accelerate your CMMC certification journey with expert guidance, we offer:

Free 30-Minute Gap Analysis Call

- Review your current compliance posture
- Identify your biggest gaps
- Get a custom 90-day roadmap
- Understand costs and timeline for your situation

Email us: ryan@blackhawkmsp.com **Call us:** 1 (925) 218 - 4000

BOOK NOW

PROTECT YOUR DEFENSE CONTRACTS

UNLOCK NEW OPPORTUNITIES

ACHIEVE CMMC COMPLIANCE

SCHEDULE YOUR FREE GAP ANALYSIS:
https://blackhawkcomputers.com/bookings

BLACKHAWK
IT COMPUTER
SUPPORT

Blackhawk Computer Support

✉ ryan@blackhawkmsp.com

☎ 1 (925) 218 - 4000

🌐 blackhawkcomputers.com