



AG GRACE INC



Simplify Your CMMC Journey



CMMC Documentation Bundle: What You Need Before an Assessment

You've done the self-assessment. You've built your POA&M. But before any CMMC assessor shows up (virtually or in person), there's one more crucial step: getting your documentation in order.

Why? Because even if your controls are in place, if you can't prove it, you can't pass

Your CMMC Documentation Bundle Checklist

Below are the core documents assessors expect to see. Miss one, and your audit could stall – or fail.

1. System Security Plan (SSP)

Your foundational document. It details:

- Your system boundaries
How each NIST 800-171 control is implemented
Key personnel and security roles
Tip: Align this tightly with your data flow diagram and POA&M.

2. Plan of Action & Milestones (POA&M)

Your active roadmap for resolving known gaps:

- Each incomplete control
Assigned owners and due dates
Realistic, tracked remediation tasks

3. Data Flow Diagram (DFD)

Shows where CUI/FCI enters, exits, and flows through your system. It supports:

- Scoping
Network boundary definition
Identifying trust zones and external interfaces

4. Policies & Procedures

You'll need documented policies that reflect actual practices:

- Access Control
Incident Response
Configuration Management
Media Protection
Personnel Security
Make sure these are approved, version-controlled, and enforced.

5. Evidence Artifacts

Assessors want proof – not promises. Have ready:

- Security awareness training records
Screenshots of MFA implementation
Audit logs
Vendor contracts or SLAs
Change management tickets

6. Asset & Inventory Lists

Required for identifying system components:

- Hardware inventory
Software inventory
Cloud assets
Include version numbers, locations, and ownership if possible.

7. SPRS Submission Confirmation

If applicable, have proof of your self-assessment score uploaded to the Supplier Performance Risk System (SPRS).

Final Reminder:

CMMC compliance is not just about what you do – it's about how well you can prove it. Your documentation tells your compliance story.

Want a downloadable CMMC documentation checklist? Click here to request yours, or schedule a readiness review with our team.

Stay documentation-ready, AG Grace, Inc. Cybersecurity Consultant | CMMC Specialist

Next in the Series:

"Creating a Secure CUI Environment: What the Enclave Approach Looks Like" – Coming soon!



We are pleased to offer AG Grace Virtual Chief Information Security Officer Services

Virtual CISO Services AG Grace, Inc

With over 20 years of experience in cybersecurity, risk management, regulatory compliance, and IT program leadership, we help organizations establish and maintain mature cybersecurity programs—without the cost of a full-time CISO.

Core vCISO Services

1. Security Program Strategy & Roadmap

- Build and align cybersecurity plans with business goals
Develop multi-year roadmaps using frameworks like NIST, CMMC, HIPAA, COBIT, ISO 27001, etc.

2. Risk Management & Compliance Readiness

- Perform gap assessments and POA&Ms
Prepare for audits (CMMC, HIPAA, DFARS, SOC2)
Create risk registers and business-aligned security metrics

3. Policy Development & Governance

- Author and update security policies, procedures, and standards
Guide executive risk decisions and governance structure

4. Incident Response & Business Continuity

- Develop and test IR and BCDR plans
Lead tabletop exercises and simulate breach scenarios

5. Vendor & Third-Party Risk Management

- Evaluate supplier risk and compliance
Assist with due diligence during vendor onboarding

6. Training & Awareness

- Role-based cybersecurity training and phishing simulations
Executive coaching and risk briefings

Engagement Models

Fractional vCISO (Monthly Retainer)

Ongoing advisory and leadership services for a monthly fee

Compliance Readiness Package

Flat-fee engagements to get you audit-ready for HIPAA, CMMC, or NIST 800-171

Risk & Incident Response Assessments

One-time engagements to assess IR plans, test response, or build documentation

Board & Executive Briefings

Custom sessions to communicate cybersecurity risk in business terms

Contact:

Info@aggrace.com

www.aggrace.com | 240-315-6828

Let's secure your future—strategically.



5257 Buckeystown Pike, Suite 206, Frederick, MD 21704
Copyright © 2025 All rights reserved

No longer want to receive these emails? unsubscribe
AG Grace, Inc. www.aggrace.com