



AG GRACE INC



Simplify Your CMMC Journey



POA&M: Your Cybersecurity Action Plan, Not Just a Paper Trail

If your CMMC self-assessment turned up gaps — that's expected. What matters is what you do next.

Enter the **Plan of Action & Milestones (POA&M)** — a structured, prioritized list of steps your organization will take to close compliance gaps. It's **required** for CMMC Level 2, and it's a key part of proving you're actively working toward full implementation.

Think of it as your **remediation playbook** — and assessors will absolutely expect to see it.

What Is a POA&M?

A POA&M is a formal document that outlines:

- Which controls you don't fully meet
- Why those gaps exist
- What you plan to do about them
- Who is responsible
- When you expect to fix them

What to Include in Every POA&M Entry

- Control Reference:**
The specific NIST 800-171 or CMMC requirement (e.g., 3.1.1 - Access Control)
- Weakness Description:**
What's missing or noncompliant? Be specific, not vague.
- Root Cause (Optional but Smart):**
Helps clarify why the issue exists and informs better solutions.
- Remediation Plan:**
What you're doing to fix the issue (tools, process changes, upgrades).
- Resources Required:**
Budget, staff, tools — what's needed to complete remediation.
- Milestones & Deadlines:**
Dates for each remediation step. Don't say "ASAP" — be realistic.
- Responsible Party:**
Name the team or person who owns the task.
- Status:**
Track progress: Open, In Progress, Completed, Deferred.

Best Practices for POA&M Success

- Be Actionable:**
Every entry should read like a task list — not a wish list.
- Be Realistic:**
Don't say you'll implement a new SIEM in 2 weeks if you haven't started vendor selection.
- Tie It to Your SSP:**
Cross-reference each entry to your System Security Plan. This shows alignment and makes audits smoother.
- Keep It Updated:**
Treat your POA&M like a live project tracker — not a dusty appendix.

What Not to Do

- ✗ Don't copy/paste vague control language into your weakness description.
- ✗ Don't leave all dates blank or set them all to the same day.
- ✗ Don't ignore "low-priority" items — assessors may not agree with your definition of low.
- ✗ Don't close out items without attaching evidence.

Pro Tip:

Include supporting documentation (e.g., ticket numbers, vendor quotes, change logs) for each POA&M milestone. It builds credibility and shows you're making real progress.

Next in the Series:

"CMMC Documentation Bundle: What You Need Before an Assessment" — Don't miss it!

Need a POA&M template or review session? [Book a free POA&M planning call](#) with our compliance experts or email solutions@aggrace.com, call 240-315-6828 or visit www.aggrace.com

Stay on track,
Cybersecurity Consultant | CMMC Specialist



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