Plan of Action & Milestones

CMMC Level 2 Starter Template

Organization: _____

Program / Contract: _____

POA&M Owner: _____

Date prepared: _____

Last reviewed: _____

How to use this template

The Plan of Action and Milestones (POA&M) tracks gaps in your control implementation with remediation owners, target dates, and evidence. Per NIST SP 800-171 §3.12.2 and the CMMC scoring methodology, your POA&M is what assessors review to decide whether you're managing your gaps actively or just listing them.

> **What assessors actually look for:**
> 1. **Specific milestones.** "Implement MFA by Q4" gets flagged. "MFA enabled for all VPN users by 2026-09-30" passes.
> 2. **Named owners.** A role title is fine ("IT Manager"), but the role must map to a real person.
> 3. **Realistic + recent dates.** Target dates that already passed without remediation get flagged faster than missing dates entirely.
> 4. **Evidence of progress.** Ticket IDs, change requests, or commit messages tied to the gap.
> 5. **Closeout discipline.** Closed entries should reference the artifact that proves closure (audit log, config screenshot).

Rules from the DoD Assessment Methodology v1.2.1

- You cannot POA&M your way through an assessment. Certain high-impact controls (3.1.1, 3.1.2, 3.5.3, etc.) MUST be implemented; gaps on these block certification.
- Total POAM-eligible deductions are capped. If your SPRS score is below the contract threshold, no amount of POA&M entries will save you.
- Assessment-time POAMs have a **180-day closeout window**. After 180 days, the gap is treated as unremediated.

POA&M Entries

ENTRY ID	CONTROL	GAP DESCRIPTION	RISK	OWNER	TARGET DATE	STATUS	EVIDENCE / NOTES
P-001	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-002	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-003	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-004	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-005	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-006	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-007	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-008	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-009	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-010	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-011	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-012	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	

ENTRY ID	CONTROL	GAP DESCRIPTION	RISK	OWNER	TARGET DATE	STATUS	EVIDENCE / NOTES
P-013	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-014	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-015	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-016	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-017	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	
P-018	*3.X.X*		*H / M / L*		*YYYY-MM-DD*	*Open*	

Example entries

Below are three example POA&M entries that would pass an assessor's specificity check.

ENTRY ID	CONTROL	GAP DESCRIPTION	RISK	OWNER	TARGET DATE	STATUS	EVIDENCE / NOTES
P-001	3.5.3	MFA enforced for admin accounts only; standard users on SSO without MFA.	High	IT Director (J. Smith)	2026-09-30	In progress	Okta tenant config in change ticket #4821. MFA rollout phased by department; Engineering done 2026-06-15.
P-002	3.13.11	VPN uses TLS 1.2 but not FIPS-validated cryptographic module.	Medium	Network Lead (M. Cruz)	2026-11-15	Open	Vendor patch ETA Q3 2026. Tracked in vendor support case 18372. Compensating control: dedicated VLAN for CUI traffic.
P-003	3.6.2	Incident response plan exists but has not been tabletop-tested in last 12 months.	Low	Compliance Lead (A. Park)	2026-08-15	In progress	Tabletop scheduled for 2026-08-12 with full IR team. Will publish report by 2026-08-20.

What to copy from these examples:

- Gap descriptions name the SPECIFIC deficiency (not the control as a whole).
- Owners include the human name in parentheses.
- Evidence references concrete artifacts (ticket IDs, vendor case numbers, schedule dates).
- In-progress entries describe the state of remediation, not just "working on it."

Maintenance discipline

A POA&M is only useful if it's current. Review at least quarterly:

- Update status of every open entry. Push dates back only with a written reason.
- Close entries with explicit evidence (audit log, screenshot, config diff).
- Add new entries promptly when gaps are discovered. Adding gaps late is what makes auditors question whether the POA&M reflects reality.
- Archive closed entries, but keep them accessible for at least 3 years (or as long as your contract requires).

Need help maintaining this?

Readyline GRC tracks POA&M entries against your control implementations + auto-ages open entries with reminders to owners. It exports back to this same shape (or OSCAL JSON for primes that consume it).

readylinegrc.com · **hello@readylinegrc.com** · Cipher One Tech LLC · Maryland, USA