

POA&M

Avalon turns a POA&M backlog from an audit liability into a managed, evidence-backed remediation program that protects the system's authorization.

THE PROBLEM WE ADDRESS

An AO facing renewal on a system with hundreds of aged, unresourced open items has little basis to reauthorize — and ATO lapses interrupt mission systems. Weak remediation programs and stale POA&Ms are perennial findings in annual IG FISMA evaluations and GAO reviews — and they roll up to the CISO and agency head.

WHAT WE DO

- Complete entries built from findings: weakness, source, severity, assets, milestones
- Deduplication and consolidation of overlapping backlog items
- Re-scoring against CVSS, CISA KEV, and agency risk criteria
- Re-baselined milestone dates against real resource availability
- Weekly or biweekly working sessions with owner escalation
- Monthly status reporting mapped to CIO-metric language
- Per-item closure evidence packages formatted for SCA validation
- Risk acceptance memos and deviation/waiver request drafting

HOW WE DO IT

1 INTAKE & BASELINE

Access provisioning, ledger export, and a data-quality/aging analysis producing the baseline report.

DELIVERABLE

Baseline report

3 CADENCE & CLOSURE

Working-session rhythm stood up; closure evidence packages produced for validation-ready items.

DELIVERABLE

Closure evidence packages

2 RATIONALIZE & RE-BASELINE

Dedupe, re-score against current threat data, and rebuild milestones against real resources.

DELIVERABLE

Rationalized ledger

4 HANDOFF

Management SOP delivered and the government team trained on the cadence.

HANDOVER

SOP + trained team

VALUE DELIVERED

- A ledger that survives validation.** Every closure claim ties to a named artifact — configuration exports, scan deltas, change records.
- A defined exit, not open-ended staffing.** Fixed price for a bounded sprint with measurable exit criteria.
- Metrics that hold up.** Re-scored, re-baselined entries feed accurate CIO FISMA metrics instead of a stale ledger.
- Less dependence on any one contractor.** Every sprint ends in a documented SOP the government team can run itself.

THE ONE THING TO REMEMBER

A productized sprint with a defined exit, not open-ended staff augmentation.

COMMONLY PROCURED AS

POA&M management / remediation-tracking support

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	8–12 wks for a standalone cleanup sprint
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-53 (CA-5, PM-4), NIST SP 800-37 (RMF), CISA KEV Catalog, OMB M-02-01

WHO WE WORK WITH

- ISSM / CISO facing an ATO renewal with an aged POA&M backlog
- Program manager needing remediation tracked and reported accurately
- AO staff preparing CIO FISMA metrics for CyberScope submission

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

NIST SP 800-53 (CA-5, PM-4)

NIST SP 800-37 (RMF)

CISA KEV CATALOG

OMB M-02-01