

NIST RMF INTEGRATION

Avalon engineers the Risk Management Framework into how your agency builds and operates systems — control baselines built in from categorization forward, evidence generated automatically.

THE PROBLEM WE ADDRESS

New capabilities sit unauthorized for 6–18 months while operators resort to workarounds, and authorization packages go stale within a quarter of signature as posture diverges from paperwork.

IG and GAO audits routinely flag continuous monitoring and POA&M management as ineffective, and every reauthorization means rewriting the SSP from scratch because evidence was never structured to regenerate.

WHAT WE DO

- Authorization posture assessment: package age, evidence currency, open POA&M items
- FIPS 199/SP 800-60 categorization and SP 800-53B baseline tailoring
- Inheritance and common-control architecture with responsibility matrices
- Control implementation engineering matched to actual system configuration
- SDLC/DevSecOps integration with compliance-as-code (SCAP, OpenSCAP, InSpec)
- OSCAL-formatted, machine-readable artifacts where agency tooling supports them
- ISCM strategy design per NIST SP 800-137: frequencies, metrics, data feeds
- Runbooks, SOPs, and hands-on training for ISSOs and ISSMs

HOW WE DO IT

1 KICKOFF & POSTURE ASSESSMENT

Stakeholder mapping, package/GRC review, and a gap analysis against the 800-53 baseline.

DELIVERABLE

Posture + gap report

3 IMPLEMENTATION & AUTOMATION

Control implementation engineering, pipeline control gates, and compliance-as-code evidence automation.

DELIVERABLE

Automated evidence pipeline

2 FRAMEWORK STRUCTURING

Categorization validation, baseline tailoring with ODPs, and inheritance architecture approved by the ISSM/AO.

DELIVERABLE

Structured GRC record

4 OPERATIONALIZATION

Runbooks, training, an assessment-readiness dry run, and a declining-involvement handoff.

HANDOVER

Trained team + readiness dry run

VALUE DELIVERED

- › **Evidence that regenerates itself.** Compliance-as-code means evidence comes from the system, not reconstruction by hand each cycle.
- › **Engineering-first, not documentation-hours.** A senior-weighted team engineers the baseline into design and configuration, not just prose describing it.
- › **cATO-aligned where it matters.** Programs aligned to DoD's cATO Evaluation Criteria assemble the demonstration evidence an AO needs.
- › **Honest about scope.** Avalon states plainly what it does not certify, and declines the independent-assessment role on systems it engineered.

COMMONLY PROCURED AS

RMF engineering / continuous authorization support services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	4–8 months for a single Moderate-baseline system
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-37 Rev 2, NIST SP 800-53 Rev 5/53A/53B, NIST SP 800-137, DoDI 8510.01

WHO WE WORK WITH

- ISSM / AO representative needing continuous, not point-in-time, evidence
- DevSecOps / platform lead integrating compliance-as-code into a pipeline
- Program office facing a stale package ahead of reauthorization

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 800-37 REV 2

NIST SP 800-53 REV 5/53A/53B

NIST SP 800-137

DDI 8510.01

