

FISMA, FEDRAMP & NIST 800-53 COMPLIANCE AUDITS

Avalon's assessors independently verify a system's controls through document review, interviews, and hands-on technical testing — delivering the evidence your AO, IG, or FedRAMP reviewer needs.

THE PROBLEM WE ADDRESS

A system can't legally operate without a current ATO, and an ATO can't be granted without credible, independent evidence — but in-house ISSO staff are often too close to the system to assess it credibly.

Checkbox competitors deliver spreadsheet reviews with no technical verification, which assessors and auditors see through immediately.

WHAT WE DO

- Boundary and baseline confirmation with FIPS 199 review
- Documentation review of the SSP, prior SARs, POA&M, and plan set
- Control-by-control assessment using SP 800-53A examine/interview/test methods
- Authenticated scans and STIG/CIS configuration verification
- Readiness assessment against the IG FISMA maturity model's nine domains
- CIO/IG FISMA metrics gap report and readiness briefing
- Gap report against FedRAMP Rev 5 baselines or 20x Key Security Indicators
- Findings formatted for direct import to eMASS, CSAM, Xacta, or RegScale

HOW WE DO IT

1 KICKOFF & PLANNING

Boundary validation, baseline confirmation, and Security Assessment Plan drafting.

DELIVERABLE

Security Assessment Plan

2 DOCUMENTATION REVIEW

SSP, prior SAR, and plan-set review; control-by-control desk assessment.

DELIVERABLE

Desk-assessment findings

3 FIELDWORK

Interviews, evidence examination, authenticated scans, and STIG/CIS configuration checks.

DELIVERABLE

Field-verified evidence

4 REPORTING & OUTBRIEF

Finding validation, risk rating, Security Assessment Report, and executive outbrief.

HANDOVER

Final SAR + POA&M inputs

VALUE DELIVERED

- › **Findings that trace to procedure.** Every result maps to a specific SP 800-53A procedure and a specific piece of evidence.
- › **Technical testing behind the paperwork.** Results are backed by authenticated scanning and STIG/CIS configuration testing, not just interviews.
- › **GRC-ready output.** POA&M inputs are formatted for direct import into eMASS, CSAM, Xacta, or RegScale.
- › **Engineering-literate assessors.** Digital Transformation experience means cloud architectures and CI/CD pipelines get assessed natively.

THE ONE THING TO REMEMBER

Procedure-level workpapers, not a spreadsheet review.

COMMONLY PROCURED AS

Independent security control assessment / compliance audit services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	10–12 wks for a full Moderate-baseline assessment
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-53A Rev 5, NIST SP 800-37 (RMF), FedRAMP Rev 5/20x, IG FISMA Maturity Model

WHO WE WORK WITH

- AO / ISSO needing an independent assessment ahead of a decision
- CISO staff preparing for the annual IG FISMA evaluation
- System owner or CSP sponsor needing a FedRAMP-aligned gap check

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 800-53A REV 5

NIST SP 800-37 (RMF)

FEDRAMP REV 5/20X

IG FISMA MATURITY MODEL