



Securing Tomorrow's Missions Today.



Independent Proof Your Controls Work: FISMA, NIST 800-53 and FedRAMP Assessments for Agency Buyers

FISMA, FedRAMP and NIST 800-53 Compliance Audits: an independent assessment, scheduled back from the date your authorization expires.

AvalonTechServices.com
contact@AvalonTechServices.com

Executive Summary	2
Why Assessments Slip	3
Why It Concentrates in Government	3
How the Need Sounds	3
The 2026 to 2028 Calendar	4
What the Service Does	5
Inside a Lane A Assessment	5
Independence Rules	7
Where It Fits in the Frameworks	7
Certification Covers the Offering, Not Your System	8
How an Engagement Runs	9
What the Agency Provides	9
What Is Not Included	10
How Avalon Staffs It	10
Pricing and How to Buy	12
Illustration: Back-Scheduling From ATO Expiry	12
Common Pitfalls	14
Conclusion and Next Step	14
Appendices	15
Appendix A: Glossary	15
Appendix B: Illustration Assumptions	15
Appendix C: References	16

Executive Summary

Every federal system has to show, on a recurring basis, that its security controls are in place and working. FISMA requires it, the NIST Risk Management Framework defines how, and NIST SP 800-53 supplies the controls. The proof is a Security Assessment Report (SAR) written by an assessor independent of the people who built and run the system.

In practice, that report is where schedules break. Assessments get scheduled late, evidence arrives late, and the Authorizing Official (AO) receives the package with too little time to read it. The authorization either lapses or gets extended under pressure. Meanwhile the yardsticks keep moving: FedRAMP published its Consolidated Rules on June 25, 2026, CISA replaced its vulnerability directives with BOD 26-04 on June 10, 2026, and OMB replaced M-21-31 with a risk-based logging model in M-26-14.

This paper is written for the people who buy and use an independent assessment: the CISO, the system owner or program manager, the ISSM and ISSO, the CIO and the contracting officer's representative. The AO is the report's real reader. It describes Avalon Technology Services' FISMA, FedRAMP and NIST 800-53 Compliance Audits service in three lanes:

- **Lane A: security control assessment.** One system boundary assessed against its SP 800-53 Rev. 5 baseline using SP 800-53A procedures, producing a SAR suitable for the authorization package.
- **Lane B: FISMA program readiness.** A component's assessment program reviewed against the inspector general's FISMA maturity model before the IG's own evaluation.
- **Lane C: FedRAMP gap audit or agency-side package review.** A cloud system's readiness checked against FedRAMP requirements, or a provider's package reviewed to support the agency's own risk decision.

Section 9 works through an illustrative back-schedule for a Moderate system whose authorization expires on June 30, 2027. Planning on October 1, 2026, the agency has about 10.9 weeks of float before it must start buying the assessment. Slow access and a longer AO review cut that to about 2.9 weeks, and starting procurement on February 1, 2027 leaves the final package about 6.7 weeks late.

The service assesses and reports. It does not fix findings, write the system security plan it assesses, grant an authorization or certify a cloud offering. Those decisions belong to the AO, the FedRAMP program and the inspector general.

Why Assessments Slip

Risk	How it shows up
Expired authorization	The system keeps running outside a current risk acceptance, or the AO signs a short extension with conditions because the SAR was not ready.
IG findings	The annual IG FISMA evaluation lands below "effective" in one or more domains, and the finding goes into a report the agency has to answer.
Untested controls	Controls that exist on paper are never examined or tested, so real weaknesses stay invisible until an incident.

Why It Concentrates in Government

- **The work is recurring by law.** FISMA and OMB Circular A-130 require ongoing assessment and periodic authorization, so the obligation returns every cycle whatever the budget does.
- **Independence is part of the framework.** SP 800-37 Rev. 2 expects the assessor to be independent of the people who implement the controls. An ISSO who documented the controls cannot credibly grade them.
- **Teams are thin.** Security staff are stretched across large system inventories, and 2025 and 2026 workforce reductions widened the gap.
- **The yardsticks move.** SP 800-53 now updates through continuous releases, FedRAMP was restructured in 2026, and CISA's directives changed in the same year. Keeping current is a job in itself.

How the Need Sounds

"Our ATO expires in June and we haven't started the reassessment." "The IG dinged us on the same domain again." "We're behind on our annuals." "My ISSOs would be grading their own homework." "Nobody has checked whether that cloud provider's package covers what we use it for." The scoping question for all of them is the same: when does the authorization expire, and who is your AO?

The 2026 to 2028 Calendar

Date	Event	What it means for assessments
February 2, 2022	DoD continuous ATO memorandum	Continuous authorization depends on ongoing assessment evidence, not a three-year snapshot
September 24, 2025	DoD announces the Cybersecurity Risk Management Construct (CSRMC)	RMF, DoDI 8510.01 and eMASS remain in use; assessments continue on the current process
February 6, 2026	CISA BOD 26-02 on end-of-support edge devices	Inventory within 3 months, decommission within 12, replace within 18; unsupported edge devices become assessable findings
May 2026	OMB M-26-14 replaced M-21-31	Audit and logging controls are assessed against a risk-based logging model
June 10, 2026	CISA BOD 26-04 replaces BOD 22-01 and BOD 19-02	Risk-based remediation clocks (3 days with forensic triage, 14 days, 60 days, next upgrade); policy immediately, processes within 60 days, full timelines within about 180 days
June 25, 2026	FedRAMP Consolidated Rules published	Offerings become "FedRAMP Certified" in classes A through D; annual penetration test by a FedRAMP Recognized assessor
June 11, 2027	New FedRAMP Rev5 submissions stop	Agencies relying on Rev5 packages need to understand what they are consuming
December 31, 2028	FedRAMP Rev5 authorizations end	Every Rev5-based cloud dependency needs a plan

Date	Event	What it means for assessments
September 30, each year	One-year O&M funds expire	Fixed-price assessments are commonly bought July through September

What the Service Does

Each engagement starts by naming the lane, because the yardstick, the deliverable and the price differ.

Lane	What is assessed	Yardstick	Primary output
A. Security control assessment	One defined system boundary, initial or reassessment	SP 800-53 Rev. 5 baseline plus agency overlays, assessed with SP 800-53A procedures	SAP, SAR, risk exposure table, POA&M inputs
B. FISMA program readiness	A component's assessment program across its systems	OMB guidance, CIO FISMA metrics, IG maturity model (9 domains, Levels 1–5)	Workpapers, metrics gap report, IG-readiness briefing
C. FedRAMP gap audit or package review	A cloud-bound system, or a provider's package the agency intends to rely on	FedRAMP requirements under the 2026 Consolidated Rules	Gap report and roadmap, or a package review memo

Inside a Lane A Assessment

- **Boundary and baseline confirmation.** FIPS 199 categorization, the SP 800-53 release in force and the overlays that apply, such as CNSSI 1253 for DoD or CMS ARS for health systems, written into the assessment plan.
- **Documentation review.** The system security plan, prior SARs, the POA&M, contingency plan, incident response plan and configuration management plan.

- **Control-by-control assessment.** Examine, interview and test methods from SP 800-53A, with a written procedure and an evidence reference for every control in scope.
- **Technical verification.** Authenticated vulnerability scans, configuration checks against DISA STIGs or CIS Benchmarks, and sampling of accounts, audit logs and change records.
- **Directive conformance.** Checks against CISA BOD 26-04 and BOD 26-02 where they bear on the controls being assessed.
- **Findings.** Each finding carries a risk rating, the procedure and evidence behind it, and a recommended corrective action.

Deliverable	Format	Use
Security Assessment Plan (SAP)	Agency template where one exists	Scope, methods, schedule and rules of engagement, signed before fieldwork
Security Assessment Report (SAR)	Word or PDF, plus an XLSX or CSV findings register	Per-control results with evidence references, for the authorization package
Risk exposure table	XLSX	Findings ranked by likelihood and impact
POA&M input file	Formatted for eMASS, CSAM, Xacta or RegScale	Direct import into the agency's GRC record
Executive outbrief	Slides and a live briefing	Written for the AO and CISO
Remediation roadmap	Word	Findings sequenced by risk and effort
Evidence index and workpapers	Organized digital binder	Repeatability and later scrutiny by an IG or assessor

Machine-readable OSCAL output is available on request, which matters more as FedRAMP moves toward continuous, machine-readable evidence.

Independence Rules

- Avalon never assesses a system whose documentation it wrote, whose controls it implemented, or whose findings it is contracted to fix.
- Assessors document and recommend; they do not change the assessed system, even for small findings during fieldwork.
- No payment depends on the result. The price is fixed, and nothing is tied to findings counts or outcomes.
- An organizational conflict of interest statement accompanies every proposal.

Where It Fits in the Frameworks

Framework	What this service addresses	What stays with someone else
FISMA and OMB Circular A-130	The periodic assessment of controls every agency system requires; readiness for the annual IG evaluation	The IG's statutory evaluation; the agency's own FISMA reporting
NIST RMF, SP 800-37 Rev. 2	The Assess step, Tasks A-1 through A-6, and assessment support to Monitor	Prepare, Categorize, Select and Implement; the Authorize decision, which is the AO's alone
SP 800-53 Rev. 5, 800-53A Rev. 5, 800-53B	Control-by-control assessment against the applicable baseline	Implementing controls; tailoring decisions
FedRAMP Consolidated Rules	Readiness gap audits and agency-side package review	The certification decision and the assessment of record by a FedRAMP Recognized assessor
DoD RMF, DoDI 8510.01	Assessment evidence recorded in eMASS where the agency grants access	The DoD authorization decision

In SP 800-53 Rev. 5 terms the work sits mainly in CA-2 Control Assessments, CA-5 Plan of Action and Milestones, CA-7 Continuous Monitoring, PL-2 System Security and Privacy Plans and RA-5 Vulnerability Monitoring and Scanning, with RA-3, CM-6 and SI-2 examined as part of the baseline.

Accurate	Not accurate
Independently assesses the system's controls against the applicable baseline and delivers a SAR suitable for inclusion in the authorization package presented to the AO	Gets the system its ATO
Identifies and prioritizes the deficiencies to close before an assessment of record or an IG evaluation	Guaranteed to pass
Reviews a provider's package to support the agency's own risk decision	FedRAMP certified by Avalon

Certification Covers the Offering, Not Your System

Under the 2026 Consolidated Rules, FedRAMP certification covers the cloud service provider's offering. The agency still authorizes its own system, including how it configures and uses that offering and the customer-responsibility controls the provider leaves to it. A Lane C package review answers the practical question: does the provider's package cover what this agency uses it for, and what is left for the agency to verify?

How an Engagement Runs

Phase	Weeks	What happens	Gate
Kickoff and assessment planning	1–2	Boundary validation, baseline and overlay confirmation, SAP, scan rules of engagement, evidence request list	Signed SAP and rules of engagement
Documentation review	3–4	Document review and desk assessment, control by control; interviews scheduled	Desk-review findings log
Fieldwork	5–8	Interviews (12–20 sessions), evidence examination, authenticated scans, STIG or CIS checks, sampling	Fieldwork complete, preliminary findings shared
Analysis and reporting	9–10	Findings validated with system staff, risk rating, SAR drafting, independent QA review	Draft SAR delivered
Outbrief and closeout	11–12	Agency factual-accuracy review, final SAR, POA&M input handoff, executive outbrief	Final SAR and POA&M inputs accepted

That plan is for a Moderate system of about 290 controls. An annual control subset runs 4 to 6 weeks, a Low baseline 6 to 8 weeks, a Lane B program review 8 to 12 weeks and a Lane C audit or review 4 to 8 weeks per system or package.

What the Agency Provides

- A named ISSO or ISSM point of contact with 4 to 8 hours a week available.
- Subject matter experts for interviews of 30 to 45 minutes each, typically 12 to 20 sessions for a Moderate system.
- Scan credentials and a signed rules-of-engagement document before fieldwork. No scanning starts without them.
- Read access to the system's GRC record, or an export of it.

- Evidence within 5 business days of each request. Late evidence extends the schedule without penalty to either side, and every request is logged with dates.
- Facility access or visit requests started at kickoff, where any on-site work is needed.

What Is Not Included

Included	Separate work
Assessment of implemented controls	Remediation of findings
Review of the existing SSP	Writing the SSP for the same system
Use of penetration test results where a framework requires them	Penetration testing
A SAR for the authorization package	The ATO decision, or FedRAMP certification
Readiness for the IG evaluation	The IG's statutory evaluation
POA&M inputs	Running the POA&M lifecycle

How Avalon Staffs It

Avalon takes one engagement at a time, unclassified and remote-first: one Lane A assessment at a Low or Moderate baseline, one Lane B review, or one Lane C audit. It does not perform classified assessments, FedRAMP assessments of record or IG evaluations, and it does not run concurrent engagements. Avalon has no prior federal engagements under this service. Each engagement is staffed with named personnel whose certifications and investigation level match the agency's requirements, and those personnel are listed in the proposal.

Requirement	How it is handled
Lead assessor	A senior lead holding the security credential the agency requires, such as CISSP or CGRC, named in the proposal as a condition of the engagement
DoD work	Personnel qualified under DoD 8140 for the assessor work role, at the investigation level the contract requires, as a condition of the engagement
Civilian work	Public Trust investigation at the tier the agency requires, as a condition of the engagement
Scanning tools	Licensed authenticated-scanning and configuration-checking tools in place before fieldwork, stated in the proposal
Data handling	A written statement covering where assessment artifacts are stored, how they are encrypted, how long they are kept and how they are destroyed
Insurance	Professional and cyber liability coverage at the limits the contract specifies, in place before award
Team shape	Lead assessor 0.50–0.75 FTE, one or two assessors 0.50–1.00 FTE, a technical tester at 0.25 FTE in fieldwork, and project management and QA at 0.10–0.20 FTE

Pricing and How to Buy

Engagement	Market-norm range
Annual assessment, rotating control subset, one Moderate system	\$35K–\$90K
Full assessment, Low baseline	\$45K–\$85K
Full assessment, Moderate baseline	\$90K–\$180K
Lane B FISMA program readiness review	\$60K–\$150K
Lane C FedRAMP gap audit, per cloud system	\$50K–\$130K
Lane C agency-side package review, per package	\$25K–\$60K

These are market-norm estimates for planning, not a quote. Every engagement is firm-fixed-price with milestone payments of 30, 40 and 30 percent against the signed SAP, completed fieldwork and the accepted final SAR. There is no contingency fee or savings share: an assessor paid on outcomes has an objectivity problem.

Every engagement above fits under the \$350,000 simplified acquisition threshold, so it can be bought as an open-market purchase, usually with one-year O&M funds. Purchases between the \$15,000 micro-purchase threshold and the SAT are generally set aside for small business when two or more capable small businesses are expected to compete. Where the assessment sits inside a larger A&A or operations task order, the prime can subcontract it to Avalon. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Illustration: Back-Scheduling From ATO Expiry

The figures below are a planning illustration for one Moderate system, not a quote and not a result from any engagement. The useful way to plan a reassessment is backward from the date the authorization expires, not forward from whenever the work happens to start.

The system's authorization expires on June 30, 2027, about 9 months after planning begins on October 1, 2026. The AO's office needs the final SAR and updated POA&M 6 weeks before expiry. The assessment runs 12 weeks, and buying it open-market under the SAT takes an assumed 8 weeks. About 60 evidence requests are issued; 20 percent

come back an average of 5 business days after the 5-day service level, across 6 control-family tracks worked in parallel. That adds about 2 weeks.

Milestone (base case)	Latest date
Start procurement	December 16, 2026
Assessment kickoff	February 10, 2027
Final SAR and POA&M inputs to the AO's office	May 19, 2027
Authorization expires	June 30, 2027

Scenario	Assessment weeks	AO review weeks	Latest procurement start	Float
Base case	14	6	December 16, 2026	10.9 weeks
Late evidence (40% of requests late)	16	6	December 2, 2026	8.9 weeks
Slow access and a longer AO review	18	10	October 21, 2026	2.9 weeks
Base case, procurement starts February 1, 2027	14	6	December 16, 2026	6.7 weeks short

In the base case the agency has about 10.9 weeks between the planning date and the last sensible day to start buying the assessment. Doubling the late-evidence rate costs about 2 of those weeks. Slow scan credentials (four weeks late) combined with a 10-week AO review leaves about 2.9 weeks, which is no margin at all for a holiday period or a continuing resolution.

If procurement does not start until February 1, 2027, the same base-case plan delivers a decision-ready package about 6.7 weeks after the authorization expires. The AO then chooses between a lapse and an extension granted under pressure, neither of which the assessment can fix.

The price check uses the team shape in Section 7: about 832 hours at an assumed \$180 blended rate, or \$150K, priced at a fixed \$150K. That sits inside the \$90K–\$180K Moderate band and under the SAT, with milestone payments of \$45K, \$60K, \$45K. Late evidence moves the schedule, not the price.

Common Pitfalls

Pitfall	How to avoid it
Boundary creep	The assessed boundary is a contract appendix: system name, GRC record ID and component inventory as of the SAP date. Anything else is a priced modification.
Assessment turning into remediation	Assessors document and recommend; fixes go to the agency or another provider.
Overselling the result	Use the accurate language in Section 5 in the proposal, the contract and every report.
Late evidence read as assessor delay	A 5-business-day evidence service level, a named agency contact and a dated request log.
Scanning without authority	A signed rules-of-engagement document is a hard gate before fieldwork.
Assessing against a stale catalog	The SP 800-53 release and overlays are confirmed at kickoff and written into the SAP.

Conclusion and Next Step

An authorization is only as current as the assessment behind it. The assessment has to be independent, traceable control by control, and finished early enough for the AO to read it. Most reassessment problems are scheduling problems, visible months ahead to anyone who counts backward from the expiry date.

The natural first step is a short scoping call around two questions: when does the authorization expire, and who is the AO? From there, a fixed-price assessment or a smaller Lane C package review can be scoped under the simplified acquisition threshold, with the back-schedule written into the plan. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

AO

Authorizing Official: the senior official who accepts the risk of operating a system and signs the authorization decision.

ATO

Authorization to operate: the AO's decision that a system may operate at an accepted level of risk.

eMASS and CSAM

GRC platforms used by DoD and many civilian agencies to record controls, assessments and POA&Ms.

FedRAMP Recognized assessor

An assessor recognized under FedRAMP's 2026 rules to perform assessments of record, including the annual penetration test.

POA&M

Plan of action and milestones: the record of open weaknesses, owners and target dates.

ROE

Rules of engagement: the signed authorization defining what may be scanned, when and how.

SAP

Security Assessment Plan: the scope, methods and schedule for an assessment, signed before fieldwork.

SAR

Security Assessment Report: the assessor's per-control results and findings, one of the three core authorization package documents with the SSP and POA&M.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative Moderate system. None is drawn from a specific agency or a completed engagement.

Assumption	Value	Basis
Planning date and expiry	October 1, 2026; authorization expires June 30, 2027	Planning assumption
Procurement lead time	8 weeks	Open-market purchase under the SAT; planning assumption
Assessment duration	12 weeks in five phases	Top of the 10–12 week Moderate range
AO review window	6 weeks (10 alternate)	Planning assumption
Evidence requests	60, 5-business-day service level	Planning assumption
Late evidence	20% late (40% alternate), 5 business days late on average, 6 parallel tracks	Planning assumption
Access delay	None (4 weeks alternate)	Government-furnished scan credentials and ROE
Team	Lead assessor 0.50 FTE for 12 weeks; Security control assessor 1.00 FTE for 12 weeks; Technical tester (fieldwork only) 0.25 FTE for 4 weeks; Project manager and QA reviewer 0.15 FTE for 12 weeks	Inside the staffing ranges in Section 7
Price check	\$150K fixed; \$180 an hour blended for the effort check	Inside the \$90K–\$180K Moderate band

Appendix C: References

1. **U.S. Congress**, *Federal Information Security Modernization Act of 2014*, 44 U.S.C. 3551 et seq.
<https://www.congress.gov/bill/113th-congress/senate-bill/2521>

2. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource*
<https://www.whitehouse.gov/omb/information-for-agencies/circulars/>
3. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
4. **National Institute of Standards and Technology**, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
5. **National Institute of Standards and Technology**, *SP 800-53A Rev. 5, Assessing Security and Privacy Controls*
<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>
6. **National Institute of Standards and Technology**, *SP 800-137, Information Security Continuous Monitoring*
<https://csrc.nist.gov/pubs/sp/800/137/final>
7. **National Institute of Standards and Technology**, *FIPS 199 and FIPS 200*
<https://csrc.nist.gov/publications/fips>
8. **FedRAMP**, *Program rules and documentation*
<https://www.fedramp.gov>
9. **Cybersecurity and Infrastructure Security Agency**, *Binding Operational Directives, including BOD 26-02 and BOD 26-04*
<https://www.cisa.gov/news-events/directives>
10. **Department of Defense**, *DoDI 8510.01, Risk Management Framework for DoD Systems*
<https://www.esd.whs.mil/DD/>
11. **Centre Law & Consulting**, *Inflation Updates to FAR Thresholds: What Changed on October 1, 2025*
<https://centrelawgroup.com/blog/inflation-updates-to-far-thresholds-what-changed-on-october-1-2025/>