



Securing Tomorrow's Missions Today.



From Stalled Package to Signed Decision: ATO Process Facilitation for Federal Systems

Authority to Operate (ATO) Process Facilitation: an evidence-first authorization package, built by a dedicated team and ready for the Authorizing Official's decision.

Executive Summary	2
Why Packages Stall	2
What Triggers the Work	3
How the Need Sounds	4
What Facilitation Covers, Step by Step	4
Evidence-First Documentation	5
Deliverables and Boundaries	6
What the Service Does Not Include	8
How an Engagement Runs	8
The Avalon Team	10
What the Agency Provides	10
Where Authorization Is Heading	10
What the Service Supports, and What It Does Not	11
An Illustrative Engagement: Working Back From the Expiration Date	13
What the Timeline Shows	13
Pricing and Contracting	14
How the Work Is Bought	15
Risks and How the SOW Contains Them	15
Conclusion and Next Step	16
Appendices	16
Appendix A: Glossary	16
Appendix B: Deliverable and Control Map	17
Appendix C: Illustration Assumptions	18
Appendix D: References	19

Executive Summary

Every federal information system needs an Authority to Operate (ATO) before it runs on a government network, and it needs that decision renewed to keep running. The decision belongs to a senior agency official, the Authorizing Official (AO). Getting a system in front of the AO takes a large body of documentation, evidence that the protections actually work, and months of coordination among engineers, security staff, an independent assessor and the AO's office. Most program offices cannot staff that work on top of their day jobs, so packages stall.

This paper is written for system owners and program managers whose deployments are blocked, the ISSMs and ISSOs who own packages day to day, the CISOs carrying an authorization backlog, and the contracting officers who buy the work. It describes Avalon Technology Services' ATO Process Facilitation service. Avalon acts as the system owner's authorization team:

- **Builds the package.** Categorization, boundary, control selection, the System Security Plan, the supporting plan set and the evidence library, in the agency's own governance platform.
- **Prepares the system for assessment.** A mock assessment against the NIST SP 800-53A procedures, then liaison and findings support during the independent assessment.
- **Assembles the decision.** A resourced POA&M, a residual-risk narrative and a briefing the AO can act on, followed by a continuous monitoring handoff.

The method is evidence-first: no implementation statement ships unless it traces to a named artifact, configuration export or interview record. Two boundaries are fixed. Avalon never grants or guarantees an authorization, because only the AO can decide. And Avalon never performs the independent assessment on a package it prepared.

The entry point is a fixed-price readiness review of \$15K to \$40K. Section 9 works backward from an illustrative ATO expiration of June 30, 2027. If the package has to be rebuilt, a typical schedule needed procurement to start by September 20, 2026. If the package is still serviceable, the agency has until about December 21, 2026, and pays roughly half as much.

Why Packages Stall

The authorization requirement is statutory under FISMA, and the process that implements it, NIST SP 800-37, is deliberately rigorous. Neither is going away. What makes packages stall is the way the work is staffed and sequenced.

Risk	How it shows up for an agency
Compliance	Systems running without a current ATO become IG and GAO findings, drag down annual FISMA metrics, and put the CISO and AO under audit scrutiny.
Mission	Finished capabilities sit undeployed because no one can produce the package. Expiring ATOs force extension memos or shutdown decisions on systems the mission depends on.
Operational	A package written to pass rather than to describe reality hides real weaknesses. The agency no longer knows its own risk posture.
Cost	A program blocked at the authorization gate keeps paying O&M, contractor labor and license fees while delivering no mission value.

Behind those risks sit structural causes. ISSO and ISSM positions turn over faster than packages get written. The three-year reauthorization cycle is a permanent treadmill. Legacy systems predate their own documentation. Governance platforms such as eMASS, CSAM and Xacta add a data-entry burden of their own. And every cloud migration creates a new authorization boundary faster than agency security shops can absorb it.

What Triggers the Work

- A finished capability blocked from production for lack of an ATO or an Interim Authority to Test (IATT).
- A current ATO expiring within six to nine months, or an IATT or conditional authorization nearing its end.
- An adverse or heavily caveated assessment result.
- An IG or GAO finding naming unauthorized or expired systems.
- A cloud migration or major architecture change that invalidates the existing boundary.
- A new AO who resets documentation expectations.
- Year-end funds available to burn down a backlog.

How the Need Sounds

"Our package has been sitting with the assessor for months." "We lost our ISSO and nobody owns the eMASS record." "We have four hundred open POA&M items and the IG noticed." "We're operating on an extension memo." "The system is done but security won't let us deploy." Any one of these is this service. Two or more usually means a readiness review should start within weeks.

What Facilitation Covers, Step by Step

The engagement follows the seven steps of NIST SP 800-37 Rev. 2. Avalon does the work in every step except the two that must stay independent: the assessment and the decision.

RMF step	What Avalon does
Prepare	Map stakeholders (system owner, ISSM/ISSO, AO or AODR, assessor); inventory existing artifacts; review gaps against the agency's authorization checklist; plan the work around the AO office's actual intake process
Categorize	FIPS 199 categorization with documented rationale; information types per SP 800-60; boundary definition with network and data-flow diagrams; privacy threshold analysis and, where triggered, Privacy Impact Assessment support
Select	Baseline selection (SP 800-53B, or CNSSI 1253 for national security systems); tailoring with written justification; common and inherited controls, including cloud inheritance through the customer responsibility matrix; overlays
Implement	Implementation statements that describe what is actually configured; the contingency, incident response and configuration management plans; coordination, not performance, of fixes that block documentation
Assess (support)	Mock assessment against SP 800-53A procedures; evidence library; review of the Security Assessment Plan; liaison and war-room support during the assessment; findings clarification
Authorize	POA&M with realistic milestones and resources; residual-risk narrative; package assembly in the system of record; AO briefing; responses to AO and AODR questions through the decision
Monitor (transition)	Continuous monitoring strategy per SP 800-137; control assessment calendar; handoff so the agency ISSO, or an RMF Integration engagement, can sustain the authorization

Evidence-First Documentation

Assessors do not grade prose. They test controls against the SP 800-53A procedures, and they compare what the System Security Plan says with what the system actually does. Packages fail when implementation statements are template language that

describes a control in general terms rather than the configuration in front of the assessor.

Avalon's rule is simple: no implementation statement ships unless it traces to a named artifact, a configuration export or an interview record. In practice that means three habits.

1. **Interview the engineers who run the system.** The people writing the statements can read the configurations behind them, because they come from cloud, identity and DevSecOps engineering work, not only compliance writing.
2. **Pull the evidence before writing the statement.** Configuration exports, STIG and SCAP results, access lists, change records and scan reports go into the evidence library first. The statement then cites them.
3. **Log every assumption.** When an engineer cannot confirm a setting, the statement says so and the gap goes on the tracker. Plausible fiction is how packages fail assessment.

Inherited controls get the same treatment. A cloud provider's FedRAMP authorization covers the provider's controls, not the agency's use of the service. The customer responsibility matrix records which controls are inherited, which are shared, and which the system owns, and each shared control gets the evidence for the agency's half.

Where the agency's platform accepts it, artifacts are structured in OSCAL, NIST's machine-readable format, so the package moves with the government's direction rather than against it. OMB's July 2024 FedRAMP memorandum, M-24-15, set that direction for cloud authorizations.

Deliverables and Boundaries

Deliverable	Format
FIPS 199 categorization memo with rationale	Document and governance platform entry
Boundary description, network and data-flow diagrams	Diagram source and PDF
System Security Plan with implementation statements	The agency's platform of record (eMASS, CSAM, Xacta, Archer or ServiceNow IRM); OSCAL export where supported

Deliverable	Format
Risk assessment (SP 800-30 method)	Document
Contingency plan and test report (SP 800-34)	Document
Incident response and configuration management plans	Document
Privacy threshold and impact assessment support	Agency privacy-office templates
Interconnection agreements (ISAs and MOUs)	Agency templates
Hardware and software inventory	Spreadsheet and platform entry
Readiness report from the mock assessment	Document, briefed live
POA&M with milestones, resources and dates	Platform entry and spreadsheet
AO decision briefing and executive risk summary	Briefing deck
Continuous monitoring strategy and assessment calendar	Document and calendar

What the Service Does Not Include

Excluded	Why, and where it belongs
The authorization decision	The AO grants, denies or conditions the ATO. Avalon prepares the basis for the decision.
Independent assessment of a package Avalon prepared	An agency Security Control Assessor, an independent team, or a FedRAMP 3PAO. Preparing and assessing the same package is a conflict of interest.
FedRAMP 3PAO services	Avalon is not a 3PAO and will not become one while offering preparation services.
Penetration testing	A separate assessment service, scoped and priced on its own
Hands-on remediation beyond minor fixes	Avalon's Remediation & Patch Management service, by change order or parallel task
Building or operating the system	The program and its integrator

How an Engagement Runs

An initial authorization of a Moderate-baseline system with cooperative stakeholders runs in eight phases.

Phase	Work	Duration
0. Kickoff and artifact inventory	Stakeholder map, document collection, gap review, engagement plan	2–3 weeks
1. Boundary and categorization	FIPS 199, boundary, diagrams, privacy threshold analysis	2–4 weeks
2. Control selection and tailoring	Baseline, tailoring rationale, inheritance mapping	2–3 weeks
3. Documentation and evidence	SSP authoring, plan set, evidence library (the long pole)	8–16 weeks
4. Readiness review	Mock assessment, gap burn-down, evidence fixes	2–4 weeks
5. Assessment support	Assessment plan review, liaison, war room, findings clarification	3–6 weeks (assessor-controlled)
6. POA&M and package	POA&M, residual-risk narrative, package assembly, AO briefing	2–4 weeks
7. Monitoring handoff	Strategy, calendar, handoff	1–2 weeks

An initial Moderate authorization typically takes five to nine months. A reauthorization with a serviceable existing package takes three to five. High-baseline, classified-adjacent or STIG-heavy DoD environments add 30% to 50%. The independent assessor's schedule and the AO's decision timeline are government-controlled and sit outside any contractor's period-of-performance commitment, and every SOW should say so.

The Avalon Team

Role	Responsibility	Loading
Engagement lead (senior A&A, CGRC or CISSP level)	Method, AO-office interface, quality gate on every artifact	0.5–0.75 FTE
Security controls analyst	Implementation statements, plan set, evidence library, platform data entry	1.0 FTE, phases 3–6
Technical subject-matter expert	Interviews engineers and validates statements against configuration	0.25–0.5 FTE
Project manager	Schedule, dependency tracking, status reporting	0.15–0.25 FTE

What the Agency Provides

Evidence collection is where calendars slip, so these go into the SOW as conditions, with day-for-day schedule relief when they slip:

- A named system owner sponsor with authority to compel participation, and an ISSM or ISSO counterpart available at least four hours a week.
- Engineer and administrator time for interviews and evidence pulls.
- Governance platform accounts by week three. eMASS accounts require sponsorship, training and, for DoD, CAC issuance, so the request starts at kickoff.
- Prior SSPs, assessment reports, POA&Ms, diagrams and policies.
- Scheduled checkpoints with the AO or AODR office, so expectations are set before the package arrives.

Where Authorization Is Heading

The process is moving toward continuous evidence and machine-readable packages. None of these developments removes the need for a well-built package; each changes what the package has to contain.

Development	What it means for a package
DoD continuous ATO memorandum (February 2, 2022)	A path to ongoing authorization for programs that demonstrate continuous monitoring of RMF controls, active cyber defense and an approved DevSecOps reference design. The memo states that continuous authorization can be revoked.
DoD Cybersecurity Risk Management Construct (announced September 24, 2025)	Named as RMF's successor in DoD, built on automation, continuous monitoring, inheritance and reciprocity. RMF processes, DoDI 8510.01 and eMASS remain in use while implementation guidance is issued.
OMB M-24-15 (July 2024)	Modernizes FedRAMP toward automation and machine-readable authorization packages
FedRAMP Consolidated Rules (published June 25, 2026)	Mandatory for all stakeholders from January 1, 2027. New Rev5 submissions stop June 11, 2027, and Rev5 authorizations end December 31, 2028. Cloud provider packages will change format; the agency's customer responsibility obligations do not go away.

A package built on traceable evidence carries across these changes because the evidence attaches to controls, not to a document template. Once a system is authorized, keeping that evidence current is a separate engineering job. Avalon's RMF Integration service picks up there, wiring evidence collection into the pipeline and monitoring tools so the next reauthorization is not another rebuild.

What the Service Supports, and What It Does Not

Framework or authority	What the service addresses
FISMA (44 U.S.C. § 3551 et seq.)	The statutory requirement behind the engagement; the package is the evidence base agencies report against
NIST SP 800-37 Rev. 2	Executes or supports all seven RMF steps

Framework or authority	What the service addresses
NIST SP 800-53 Rev. 5, 800-53A, 800-53B	Control documentation, tailoring and inheritance; the assessment procedures the readiness review uses
FIPS 199 and FIPS 200	Categorization and minimum security requirements
NIST SP 800-18, -30, -34, -60, -137	SSP structure, risk assessment, contingency planning, information types, continuous monitoring strategy
OMB Circular A-130	The policy that binds agencies to authorization and ongoing assessment
DoDI 8510.01 and CNSSI 1253	DoD RMF implementation and national security system categorization
FedRAMP	Advisory and package preparation for cloud offerings or agency sponsors; never 3PAO assessment
NIST SP 800-171 and CMMC	Not addressed. These govern contractor systems handling CUI, not agency system authorization.

Approved phrasing	Prohibited phrasing
"Prepares an assessment-ready authorization package"	"Delivers your ATO"
"Facilitates the RMF process through the authorization decision"	"Guarantees authorization" or "guaranteed to pass assessment"
"Reduces preparation and rework time in the authorization cycle"	"Certifies your system as compliant"
"Positions the system for the AO's risk decision"	"Avalon-issued authorization"

Avalon prepares, advises, documents and facilitates. It does not grant authorizations, does not assess packages it prepared where independence is required, does not confer FedRAMP status, and does not guarantee any assessment or authorization outcome.

Final authority always rests with the appropriate government official or accredited third party.

An Illustrative Engagement: Working Back From the Expiration

Date

The figures below are a planning illustration for one representative Moderate-baseline system, not a quote and not a result from any engagement. The system's ATO expires on June 30, 2027. The question for the program office is when the reauthorization work has to start, and the answer depends on one thing it may not yet know: whether the existing package is still serviceable or has to be rebuilt.

Phase durations come from the ranges in Section 6, using the midpoint for a typical schedule and the top of the range for a slow one. Two government-controlled steps are added as assumptions: 6 to 10 weeks to award a fixed-price task, and 4 to 8 weeks for the AO's review after the package is submitted.

Package condition and pace	Start procurement by	Start the work by	Package to the AO by	Total lead time
Rebuild, typical	September 20, 2026	November 1, 2026	June 2, 2027	9.3 months
Rebuild, slow	May 20, 2026	July 29, 2026	May 5, 2027	13.3 months
Serviceable package, typical	December 21, 2026	February 1, 2027	June 2, 2027	6.3 months
Serviceable package, slow	September 26, 2026	December 5, 2026	May 5, 2027	9.1 months

What the Timeline Shows

- A rebuild is already late.** As of September 30, 2026, a program that needs a rebuild has missed even the typical start date for a mid-2027 expiration. Its realistic choices are compressing the schedule, adding staff, or planning for an extension memo now.

- **A serviceable package buys about three months.** Typical reauthorization of a package that still describes the system can start procurement as late as December 21, 2026.
- **Waiting turns a reauthorization into a rebuild.** At market-norm midpoints, reauthorizing a serviceable Moderate package costs about \$88K, while rebuilding it costs about \$175K. The difference, about \$88K, is what a package's decay costs when no one maintains it between cycles.

A \$25K readiness review answers the one question the table cannot: which row the program is in. It takes three to five weeks and fits under the simplified acquisition threshold, so it can start on this year's money.

Appendix C lists every input. The agency's own expiration date, package condition and procurement lead time replace them during the readiness review.

Pricing and Contracting

Scope	Typical firm fixed price
Readiness review only (mock assessment and gap report)	\$15K–\$40K
Low baseline, single cloud-hosted application with strong inherited controls	\$45K–\$90K
Moderate baseline, standard major application or general support system	\$100K–\$250K
High baseline, complex enclave, or DoD environment with full STIG evidence	\$250K–\$500K+
Reauthorization with a serviceable existing package	40–60% of the initial price
ISSO-as-a-service retainer	\$10K–\$22K a month per system or small cluster

These are market-norm planning ranges, validated against the specific system and solicitation before any figure appears in a proposal.

Package work is priced firm fixed price, with milestones and written acceptance criteria for each artifact, so performance risk sits with Avalon. Assessment support whose effort depends on the volume of findings can run from a small time-and-materials pool. The

fee is never tied to the authorization outcome: no vendor controls the AO's decision, and a fee that depends on it creates an integrity problem in the package itself.

How the Work Is Bought

GSA's Multiple Award Schedule is the natural home, under the Highly Adaptive Cybersecurity Services SIN (54151HACS) that agencies use for assessment and authorization support, or the IT Professional Services SIN (54151S) when A&A is bundled into broader work. Readiness reviews and many single-package engagements fall under the simplified acquisition threshold, which rose to \$350,000 on October 1, 2025, and can be bought as open-market purchases. Operational systems usually buy this work with one-year O&M money, which is why A&A task orders cluster between July and September.

Risks and How the SOW Contains Them

Risk	Likelihood	Impact	Containment
Evidence collection and interviews slip	High	High	Client-dependency schedule in the SOW; day-for-day relief; assumption log in every status report
Platform access (especially eMASS) arrives late	High	Medium	Requests at kickoff; access dates written into the plan
Documentation work drifts into remediation	Medium	High	Deliverables enumerated; remediation beyond minor fixes by change order
The boundary grows mid-engagement	Medium	Medium	Priced boundary named in the SOW; changes by change order
Missing policies found in phase 0	Medium	Low	Scoped as a separate policy add-on, not absorbed
Compliance oversell	Low	High	Approved phrasing only; no promised outcome or AO timeline

Conclusion and Next Step

An authorization is a risk decision, and the AO can only make a good one on a package that describes the system as it actually is. Most stalled packages are not blocked by the framework. They are blocked by missing evidence, statements nobody can verify, and coordination nobody has time to run. That is work a dedicated team can take off a program office's plate.

The first step is the fixed-price readiness review: three to five weeks and \$15K to \$40K, producing a mock-assessment result, a gap report and a clear answer on whether the package needs a reauthorization or a rebuild. Avalon runs one full Moderate engagement at a time, in unclassified environments, led by senior staff. Avalon is a small business without prior federal contracts under this service and says so; the fixed-price, milestone-based structure is built to keep the agency's exposure small. To discuss a readiness review, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

AO: Authorizing Official

The senior official who accepts a system's residual risk and grants, denies or conditions its authorization.

AODR: AO Designated Representative

The official who acts for the AO in day-to-day authorization matters.

ATO: Authority to Operate

The AO's documented decision that a system may operate at an accepted level of risk.

ConMon: Continuous Monitoring

Ongoing assessment of controls and risk after authorization, per NIST SP 800-137.

CRM: Customer Responsibility Matrix

The record of which controls a system inherits from a provider and which it must implement.

CSAM / eMASS / Xacta

Governance platforms that hold authorization records; eMASS is DoD's system of record.

IATT: Interim Authority to Test

A time-limited authority to test a system in an operational environment before its ATO.

ISA / MOU

Interconnection Security Agreement and Memorandum of Understanding, which document connections between systems.

ISSM / ISSO

Information System Security Manager and Officer, who own a system's security program and day-to-day security.

POA&M: Plan of Action and Milestones

The tracked list of known weaknesses, with owners, resources and completion dates.

PTA / PIA

Privacy Threshold Analysis and Privacy Impact Assessment.

SCA: Security Control Assessor

The independent party that assesses whether controls are implemented correctly and working.

3PAO: Third Party Assessment Organization

An accredited assessor for FedRAMP cloud authorizations.

Appendix B: Deliverable and Control Map

Deliverable	RMF step	NIST SP 800-53 Rev. 5 controls
Categorization memo and boundary	Categorize	RA-2, PL-2
System Security Plan	Implement	PL-2
Risk assessment	Categorize, Assess	RA-3
Contingency plan and test	Implement	CP-2, CP-4
Incident response plan	Implement	IR-8
Configuration management plan	Implement	CM-9
Interconnection agreements	Implement	CA-3

Deliverable	RMF step	NIST SP 800-53 Rev. 5 controls
Hardware and software inventory	Implement	CM-8
Readiness report and assessment support	Assess	CA-2
POA&M	Authorize	CA-5, PM-4
Authorization package and AO briefing	Authorize	CA-6
Continuous monitoring strategy	Monitor	CA-7

Appendix C: Illustration Assumptions

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

Assumption	Value	Basis
ATO expiration	June 30, 2027	Illustrative date
Rebuild phase durations	Phases 0–6 at the midpoint (typical) or top (slow) of Section 6 ranges	Section 6
Serviceable-package reauthorization	4 months (typical) or 5 months (slow) of work	Three-to-five-month range
Procurement lead time	6 weeks (typical) or 10 weeks (slow)	Planning assumption; government-controlled
AO review after submission	4 weeks (typical) or 8 weeks (slow)	Planning assumption; government-controlled
Readiness review price	\$25K	Inside the \$15K–\$40K tier
Rebuild (initial Moderate) price	\$175K	Midpoint of \$100K–\$250K

Assumption	Value	Basis
Reauthorization price	\$88K	50% of the initial price (40–60% range)
Excluded	Assessment fees, remediation, extension memo costs	Outside the engagement

Appendix D: References

1. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*, December 2018
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
2. **National Institute of Standards and Technology**, *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>
3. **National Institute of Standards and Technology**, *SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011
<https://csrc.nist.gov/pubs/sp/800/137/final>
4. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource*
<https://www.cio.gov/policies-and-priorities/circular-a-130/>
5. **Office of Management and Budget**, *M-24-15, Modernizing the Federal Risk and Authorization Management Program*, July 2024
<https://www.whitehouse.gov/omb/information-resources/guidance/memoranda/>
6. **Department of Defense CIO**, *Continuous Authorization to Operate (cATO) memorandum*, February 2, 2022
<https://dodcio.defense.gov/Portals/0/Documents/Library/20220204-cATO-memo-Signed-Cleared.pdf>
7. **Akin Gump**, *Department of Defense Launches CSRMC: A New Cybersecurity Risk Management Construct*, October 2, 2025
<https://www.akingump.com/en/insights/alerts/department-of-defense-launches-csrmc-a-new-cybersecurity-risk-management-construct>
8. **Cloud Security Alliance**, *FedRAMP's Consolidated Rules for 2026: The Rev5 Sunset*, July 2026
<https://labs.cloudsecurityalliance.org/research/csa-research-note-fedramp-20x-consolidated-rules-transition/>
9. **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/>