



Securing Tomorrow's Missions Today.



Out of the Data Center, On Schedule: Fixed-Price, Wave-Based Cloud Migration for Federal Agencies

Cloud Migration & Development: a fixed-price, wave-by-wave plan with the security evidence built in.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Legacy Infrastructure Is the Real Cost Driver	3
The Events That Force the Decision	3
Why Cloud Pricing Is No Longer the Main Objection	4
What the Mandates Assume	4
What the Engagement Delivers	4
Scope of Work	5
The Seven Dispositions	6
Deliverables	7
What This Service Does Not Include	7
How Delivery Works: Seven Phases, Fixed Price per Wave	8
The Avalon Team	10
What the Agency Provides	10
Security and Authorization: Evidence, Not Promises	11
How the Work Maps to Federal Frameworks	12
What Avalon Does and Does Not Certify	13
Pricing and Contracting	13
What Moves the Price	14
How the Assessment Fits the Budget Calendar	14
An Illustrative Five-Year Cost Model	14
The Representative Portfolio	14
Five-Year Comparison	15
Sensitivity: When the Case Weakens	16
Risk Register	17
Acquisition Pathways	18
Common Failure Points and How the Plan Prevents Them	19
Questions Agencies Ask	20
Where Migration Leads Next	20
Conclusion and Next Step	21
Appendices	22
Appendix A: Glossary	22
Appendix B: Compliance Mapping	23
Appendix C: Cost-Model Assumptions	25
Appendix D: References	27

Executive Summary

Most federal IT dollars never reach modernization. GAO reports that the government spends more than \$100 billion a year on IT and cyber investments and that agencies typically put about 80 percent of it toward operating and maintaining existing systems (GAO-25-107795, July 2025). The same report found that only 3 of the 11 most critical legacy systems it reviewed had fully documented modernization plans. The money, the mandates and the risk all point the same way: out of aging data centers and into authorized cloud environments. What most agencies lack is the engineering capacity to make the move without disrupting the mission.

This paper is written for the people who own that problem: agency and component CIOs, program and mission-system owners, CISOs and ISSMs, cloud program offices, and the contracting officers who buy the work. It describes how Avalon Technology Services delivers Cloud Migration & Development: the planned move of an agency's existing applications, databases and workloads into a FedRAMP-certified cloud environment, plus the code remediation needed to make those systems run properly once they arrive.

The engagement is built around four commitments:

- **Fixed price per wave.** A fixed-price assessment produces a signed application-by-application disposition list. Each migration wave after that is priced as a fixed-price scope. Time-and-materials is reserved for code remediation whose condition cannot be known up front.
- **Senior engineers doing the work.** A founder-level cloud architect leads delivery, with two to three migration engineers and one to two remediation developers.
- **Security evidence as a deliverable.** The same team that writes the infrastructure-as-code produces control implementation evidence mapped to NIST SP 800-53, packaged for the agency's own assessment and authorization.
- **Honest capacity.** Avalon takes on one small-to-mid unclassified migration at a time (roughly 5 to 25 applications, civilian or DoD IL2/IL4) and says so in writing.

Section 7 presents an illustrative five-year cost model for a representative 30-application portfolio. Under its stated assumptions, the migration costs \$2.23M less than the status quo over five years (net present value \$2.14M at the OMB Circular A-94 real discount rate) and pays back in Year 2. The model also shows the case that does not

work: when no hardware refresh or licensing event falls inside the five-year window, the savings roughly break even. That is why the fixed-price assessment compares both cost paths for the agency's actual portfolio before a single migration dollar is obligated.

Why Legacy Infrastructure Is the Real Cost Driver

Legacy infrastructure rarely fails all at once. It gets more expensive, harder to staff and harder to secure every year, until a single event forces a decision. Four kinds of risk converge on it.

Risk	How it shows up at an agency
Cost	Operations and maintenance consume most of the IT budget. Hardware refresh cycles and post-acquisition licensing changes (VMware under Broadcom is the current example) produce sudden, unbudgeted six- and seven-figure bills.
Mission	Fragile systems with single points of failure, limited disaster recovery and hardware past end of support put beneficiary-facing and warfighter-facing services at risk of outage.
Compliance	Zero trust architecture, the event logging OMB M-26-14 asks agencies to plan for, and continuous monitoring are difficult or impossible on legacy platforms. Audit and IG findings accumulate against systems that cannot be patched or instrumented.
Staffing	The people who understand these systems are retiring or have left, and recent federal workforce reductions make people-intensive legacy operations harder to sustain.

The Events That Force the Decision

In practice, migration starts when one of these lands on a program manager's or CIO's desk:

- A hardware refresh or data center lease renewal quote, often the first honest total-cost number leadership has seen.
- A software licensing repricing, such as a virtualization renewal that arrives at a multiple of last year's price.
- End-of-support dates for operating systems or databases in the environment.

- An IG or GAO finding, a failed audit, or an ATO at risk of lapsing because assessors flagged the platform itself.
- A zero trust milestone the legacy environment cannot meet. DoD components must reach target-level zero trust by the end of FY2027.
- New money or new access, such as cloud modernization credits or year-end funds that can cover a fixed-price assessment or a first wave.
- A workforce event: the last administrator who understood the system leaves.

Why Cloud Pricing Is No Longer the Main Objection

GSA's OneGov program has negotiated government-wide terms with the major cloud providers. The AWS agreement, announced August 7, 2025, provides up to \$1 billion in incentive credits across federal civilian agencies, including modernization and training credits, through December 31, 2028. Credits like these lower the agency's consumption bill without touching the migration services price, which is why Avalon checks credit eligibility during every assessment. The remaining constraint for most agencies is engineering capacity, not cloud pricing.

What the Mandates Assume

Executive Order 14028 (as amended by EO 14306 in June 2025), the federal zero trust strategy in OMB M-22-09, and the risk-based logging model in OMB M-26-14, which replaced M-21-31 in May 2026, all assume modern, instrumented infrastructure. Identity federation, micro-segmentation and centralized logging are native to a well-built cloud landing zone and very hard to retrofit onto a legacy data center. For many agencies, migration is the practical first step toward meeting these requirements.

What the Engagement Delivers

Cloud Migration & Development has two halves. The infrastructure half moves workloads into the target environment. The development half fixes what breaks when they get there: hard-coded addresses and file paths, unsupported dependencies, integrations, authentication and build pipelines. Moves that skip the second half are how agencies end up with systems that technically run in the cloud and cost more than they did on premises.

Scope of Work

1. **Portfolio discovery and assessment.** Automated and interview-based inventory of applications, servers, databases and dependencies, including licensing, data sensitivity (CUI, PII, PHI) and ATO boundaries.
2. **Per-application disposition.** Each application is assigned one of the seven standard strategies below. The agency signs the list, and it becomes the contractual scope for the rest of the engagement.
3. **Landing zone build or validation.** Account structure, identity federation, network segmentation, logging, guardrails and encryption baselines, implemented as infrastructure-as-code. If the agency already has an enterprise landing zone, this step validates it rather than rebuilding it.
4. **Wave planning.** Applications are grouped by dependency, risk and mission calendar, so no benefits system is cut over during open season, no financial system at fiscal year-end and no command system during an exercise.
5. **Migration execution.** Rehosting with replication tooling such as AWS Application Migration Service and Azure Migrate, replatforming onto managed database and container services, and targeted refactoring where the disposition calls for it. Database migration and reconciliation testing run as their own workstream.
6. **Development and remediation.** Code changes, containerization where appropriate, rebuilt interfaces, authentication moved to the agency's identity provider, and pipelines for anything that now deploys as code.
7. **Cutover, validation and hypercare.** Rehearsed cutovers with rollback plans, validation against written acceptance criteria, and a defined hypercare window with Avalon engineers on call.
8. **Security documentation throughout.** Control implementation evidence, updated architecture diagrams and configuration baselines, packaged for direct use by the agency's ISSO and assessors.

The Seven Dispositions

Strategy	What it means	Typical use
Rehost	Move the workload as-is to cloud infrastructure	Stable applications with no near-term change planned
Replatform	Move with targeted changes, such as a managed database	Applications that benefit from managed services without a rewrite
Refactor	Change the code or architecture to run cloud-native	A small number of high-value applications; larger portfolios move to Application Modernization
Repurchase	Replace with a SaaS product	Commodity functions such as ticketing, HR or collaboration
Retire	Turn it off	Duplicate or unused applications found in discovery
Retain	Leave it where it is for now	Systems with a pending decision, a hard dependency or a separate modernization path
Relocate	Move a virtualized environment without changing it	Bulk moves of a virtualization estate as a bridge step

Deliverables

Deliverable	Format
Application portfolio assessment and disposition report	Written report plus a spreadsheet inventory the agency keeps
Migration strategy and wave plan	Written plan with schedule, dependency map and risk register
Landing zone and environment configuration	Infrastructure-as-code repository (Terraform or cloud-native templates) turned over to the agency
Migrated, validated workloads	Operating systems in the target environment, accepted against written criteria
Cutover runbooks and rollback plans	Step-by-step runbooks, one per wave
Security control implementation evidence	Control-mapped package formatted for the agency's SSP and assessment
As-built architecture documentation	Diagrams and narrative, delivered at closeout
Knowledge transfer	Working sessions with agency staff, recorded where permitted, plus written operating procedures

What This Service Does Not Include

Clear boundaries protect the agency's budget and schedule as much as Avalon's. These items are deliberately outside the migration scope:

Not included	Where it belongs instead
Issuing or guaranteeing an ATO, or performing the independent control assessment	The agency's assessors and Authorizing Official; Avalon's ATO Process Facilitation service can support the process
Rewriting a major application portfolio	Application Modernization, scoped and priced separately
Building new applications	Cloud Native Development
24/7 operations and monitoring after hypercare	Enterprise Monitoring or a separate O&M task
Post-migration cost optimization and spend governance	FinOps, the natural follow-on
Designing the target architecture from scratch	Cloud Architecture & Engineering; an existing architecture is validated, not rebuilt
The cloud provider's own FedRAMP status	The provider and the FedRAMP program; Avalon lands workloads only in already-certified environments

How Delivery Works: Seven Phases, Fixed Price per Wave

The phase plan below assumes a small-to-mid unclassified portfolio of roughly 10 to 25 applications. A pilot wave proves the pattern and calibrates the estimates before the production waves commit.

Phase	Activities	Duration
0. Kickoff and access	Accounts, network access, security paperwork, stakeholder map, data call issued	1–2 weeks
1. Discovery and assessment	Inventory, dependency mapping, disposition workshops, sensitivity classification	3–6 weeks
2. Planning and landing zone	Wave plan, target architecture validation or build, infrastructure-as-code baseline, runbook templates	4–8 weeks (overlaps Phase 1)
3. Pilot wave	One to three low-risk applications migrated end to end	4–6 weeks
4. Production waves	Remaining waves in sequence; remediation development runs in parallel	8–24+ weeks, depending on portfolio
5. Cutover and hypercare	Per-wave cutover and validation, with 2–4 weeks of hypercare per wave	Runs alongside Phase 4
6. Closeout and transition	As-builts, security evidence package, knowledge transfer, decommissioning support	2–3 weeks

Total duration scales with application count, data volume, the number of interfaces per application and, above all, the agency's own change-control and testing pace. As a planning guide, 5 to 15 applications take about four to six months, and 15 to 50 applications take six to twelve months. Portfolios of more than 50 applications, or any classified or IL5+ scope, run 12 to 24 months or more and should be structured with option years.

The Avalon Team

Role	Involvement
Cloud technical lead and architect (founder-level)	Full-time through the pilot wave, then 50–75%
Migration engineers (2–3, depending on wave size)	Full-time during the pilot, production waves and cutover
Remediation developers (1–2)	As dispositions require, during production waves and cutover
Compliance specialist (ISSO support)	25–50%, concentrated in discovery, planning and evidence packaging
Project manager	25–50% throughout

What the Agency Provides

Agency-side dependencies are the most common reason migrations slip. Each item below goes into the statement of work as a government-furnished item with a named owner and a date:

- System owner and subject-matter expert time for discovery interviews and acceptance testing.
- Network and system access, plus cloud account provisioning, within the first two weeks.
- Existing documentation at kickoff: current SSPs, network diagrams and interface agreements.
- A working change-control path with agreed turnaround times.
- Funded cloud consumption in the agency's own accounts. Avalon does not resell cloud capacity.
- Timely government decisions at each wave gate.

Security and Authorization: Evidence, Not Promises

A migration changes the system boundary, so the agency will reassess and reauthorize the system in its new environment. Avalon's job is to make that reassessment faster by producing control implementation evidence as a normal output of the engineering work, not as a paperwork exercise after the fact.

Stated precisely: **Avalon migrates the system into a FedRAMP-certified environment at the required baseline and delivers control implementation evidence mapped to NIST SP 800-53, reducing the documentation lift for the agency's assessment and authorization.**

How the Work Maps to Federal Frameworks

Framework	How the migration maps to it
FISMA and NIST RMF (SP 800-37)	Migration work sits in RMF Step 3 (Implement) and produces the evidence Step 4 (Assess) uses. Assessment and authorization remain the agency's steps.
NIST SP 800-53 Rev. 5	Landing zone and workload configuration implement customer-responsibility controls, most heavily in the AC, AU, SC, CM, CP and IA families. Evidence identifies which controls are inherited from the cloud provider and which the agency implements, using the provider's customer responsibility matrix.
FedRAMP	Workloads land only in FedRAMP-certified offerings at the required baseline. Under FedRAMP's 2026 Consolidated Rules, the program is moving from "authorized" to "certified" terminology, with lettered classes replacing Low, Moderate and High (Moderate becomes Class C); the underlying control baselines do not change.
DoD Cloud Computing SRG	For DoD work the target environment must hold the right DISA provisional authorization for the impact level. Avalon's current delivery scope covers IL2 and IL4.
Zero trust (EO 14028, OMB M-22-09, DoD ZT Strategy)	Identity federation, segmentation and centralized logging are built into the landing zone, giving the agency a practical starting point for its zero trust milestones.
OMB M-26-14	A centralized log architecture in the landing zone is how agencies reach the EL1 to EL3 event logging tiers.
NIST SP 800-171	Avalon safeguards any CUI it receives during the engagement under SP 800-171. This service does not deliver CMMC certification to anyone.

What Avalon Does and Does Not Certify

Avalon performs migration engineering, security hardening and documentation. Avalon does not certify compliance, does not perform the independent assessment, and does not issue or guarantee an ATO. FedRAMP certification belongs to the cloud provider under the FedRAMP program, and the authorization decision rests with the agency's Authorizing Official. After migration, three things still require separate work: the independent control assessment, the Authorizing Official's risk acceptance and ATO decision, and ongoing continuous monitoring.

Pricing and Contracting

Federal migrations are usually priced three ways at once: a fixed-price assessment, fixed-price execution per wave, and time-and-materials for remediation development where code condition cannot be known in advance. Avalon uses that structure and treats fixed price per wave as the default, because it pays for finished waves, not billed hours.

Scope tier	Typical portfolio	Typical total price
Assessment and migration plan (entry engagement)	Up to about 50 applications inventoried and dispositioned	\$50K–\$150K, firm fixed price
Small migration	5–15 applications, unclassified	\$250K–\$900K
Mid migration	15–50 applications, mixed complexity	\$900K–\$3M
Large or multi-year	50+ applications, or IL5+ or classified scope	\$3M–\$10M+, with option years

These are market-norm planning ranges. Every figure is validated against the specific portfolio during the assessment before it appears in a proposal.

Per-application yardsticks help agencies sanity-check a quote: a simple rehost typically runs \$15K to \$75K, a replatform \$50K to \$150K, and a targeted refactor \$150K to \$500K or more. A portfolio full of refactors is an Application Modernization engagement and is priced separately.

What Moves the Price

- **Up:** more applications and interfaces, large data volumes with short migration windows, IL4 or higher requirements, database engine conversions, mainframe or unusual source platforms, slow change control, and weekend-only or 24/7 cutover windows.
- **Down:** an existing, healthy enterprise landing zone, a high share of rehosts, a consolidated source technology stack, and cloud provider modernization credits that offset the agency's consumption costs.

How the Assessment Fits the Budget Calendar

Migration of existing systems is funded mostly with one-year O&M money. That creates two natural buying windows: the second and third quarters, when spend plans firm up, and the fourth-quarter obligation window before September 30. A fixed-price assessment is a clean fit for either. It is firm fixed price, quick to award and severable from the larger effort, and it produces the disposition list that defines and de-risks every wave that follows.

An Illustrative Five-Year Cost Model

This is an illustration, not a quote and not a result. It models a representative, unclassified portfolio of 30 applications so that agencies can see how the cost components interact. Every input is listed in Appendix C, and every figure is recalculated from those inputs. The assessment replaces these assumptions with the agency's own numbers.

The Representative Portfolio

Of the 30 applications, the disposition workshops in this example retire 4, move 3 to SaaS, rehost 12, replatform 8, refactor 2 and retain 1 on premises. Avalon's services for this scope total \$2.04M, inside the mid-migration band above:

Avalon service component	Price
FFP assessment and migration plan	\$85K
Landing zone validation, pilot wave setup and evidence packaging	\$210K
Rehost waves (12 apps x \$40K)	\$480K
Replatform waves (8 apps x \$95K)	\$760K
Targeted refactor, T&M ceiling (2 apps x \$250K)	\$500K
Total Avalon services	\$2,035K

Five-Year Comparison

The status quo keeps the legacy environment running at \$3.40M a year and pays a \$2.40M hardware refresh in Year 1. The migration path pays for Avalon's services, the agency's own program costs and a year of dual running, then runs at \$2.79M a year from Year 2. Figures are in constant FY2026 dollars, in millions.

Year	Status quo	Avalon services	Agency program costs	Run costs (legacy + cloud)	Migration path total	Cumulative difference
Year 1	5.80	2.04	0.80	3.17	6.01	-0.21
Year 2	3.40	0.00	0.00	2.79	2.79	0.40
Year 3	3.40	0.00	0.00	2.79	2.79	1.01
Year 4	3.40	0.00	0.00	2.79	2.79	1.62
Year 5	3.40	0.00	0.00	2.79	2.79	2.23
Total	19.40	2.04	0.80	14.34	17.17	2.23

What the model shows

- **Five-year difference:** \$2.23M lower cost on the migration path (\$19.40M versus \$17.17M).
- **Net present value:** \$2.14M, discounted at 1.3%, the 5-year real rate in OMB Circular A-94 Appendix C for 2026, with a mid-year convention.
- **Payback:** the cumulative difference turns positive in Year 2. Year 1 costs slightly more than the status quo because of dual running and one-time program costs.
- **Run rate:** annual run cost falls from \$3.40M to \$2.79M, driven by retired applications, released sustainment staff and dropped virtualization licensing.

Sensitivity: When the Case Weakens

A model is only useful if it shows where it breaks. Each row changes one assumption and leaves the rest at the base case.

Scenario	5-year difference	NPV (1.3%)	Payback
Base case	\$2.23M	\$2.14M	Year 2
Cloud consumption 30% higher	\$0.74M	\$0.70M	Year 3
Only 2 sustainment FTE released	\$0.91M	\$0.87M	Year 2
Avalon services 25% higher	\$1.72M	\$1.63M	Year 3
No hardware refresh due in the window	-\$0.02M	-\$0.10M	Beyond Year 5
CSP modernization credits of \$250K applied	\$2.48M	\$2.39M	Year 1

Two findings matter most. First, the case depends heavily on a trigger event: if no hardware refresh or licensing repricing falls inside the window, the migration roughly breaks even over five years and the argument rests on risk, compliance and staffing rather than cost. Second, the savings are sensitive to how many sustainment staff the agency actually redeploys and to post-migration cloud governance, which is why cost governance (FinOps) is the recommended follow-on.

Risk Register

ID	Risk	Likelihood	Impact	Mitigation built into the plan
R-1	Agency SMEs, access or test staff are unavailable when a wave needs them	High	High	Government-furnished items with owners and dates in the SOW; readiness checklist at every wave gate; schedule relief tied to missed dates
R-2	Rehosts quietly turn into refactors mid-wave	Medium	High	Signed disposition list is contractual scope; changes go through a written change process; extra refactors are quoted separately
R-3	Data migration takes longer than the compute move	Medium	High	Database migration estimated as its own workstream; replication and reconciliation testing rehearsed in the pilot wave
R-4	Cutover disrupts a mission-critical period	Low	High	Wave plan built around the mission calendar; rehearsed cutover with a tested rollback plan
R-5	Cloud consumption exceeds the estimate	Medium	Medium	Rightsizing during replatform; tagging and budgets in the landing zone; FinOps review at closeout
R-6	Reauthorization of the new boundary stalls	Medium	Medium	Early engagement with the Authorizing Official; control evidence delivered wave by wave, not at the end
R-7	No one owns operations after hypercare	Medium	Medium	Operations plan agreed in the first conversation; transition-to-O&M plan attached to closeout

Acquisition Pathways

Cloud migration services are bought through a handful of pathways. The table below states plainly which ones Avalon can use directly and which it would reach through a prime.

Vehicle	Relevance to cloud migration	Avalon's access
GSA Multiple Award Schedule (SIN 518210C Cloud Professional Services; 54151S IT Professional Services)	The main pathway for civilian migration task orders and BPA calls	Priority vehicle Avalon is pursuing
NASA SEWP VI	Contract period starts November 1, 2026; Categories B and C cover IT services, and all categories support small business set-asides	Near term, as a subcontractor to Category B or C holders
OASIS+ small business pools	Services contract with continuous on-ramping; migration fits its technical domains	On-ramp candidate as Avalon's project portfolio grows
GSA Alliant 3	Large-business IT GWAC; first awards made February 2026	Subcontractor to awardees
DoD enterprise cloud contracts (JWCC)	Cloud consumption flows through the cloud provider primes	Migration services alongside consumption, on a services vehicle or as a subcontract
Small business set-asides and agency BPAs	Competitive set-asides under NAICS 541512 and 518210, and calls against agency cloud support BPAs	Direct

Contract type. Firm fixed price is the default for the assessment and each wave, because both are definable and agencies prefer fixed price for this kind of work. Time-and-materials or labor-hour fits the remediation development workstream when code condition is unknown at award. A "start small, expand competitively" strategy (a fixed-price assessment first, then waves) keeps each award small enough to move quickly.

Small business credit. Awarding directly to a small business gives the agency credit toward its small business goals, and a fixed-price assessment or first wave fits comfortably within simplified acquisition approaches. Contracting officers should confirm current thresholds, which are adjusted periodically.

Common Failure Points and How the Plan Prevents Them

Most stalled migrations trace to a short list of causes. The plan addresses each one in the statement of work, not in a slide.

Failure point	What happens	How the plan prevents it
Scope creep	"While you're in there" turns a rehost into a refactor and blows the budget	The signed disposition list is scope; every SOW states that changes to dispositions are a change in scope
Compliance oversell	A vendor implies the system will be "authorized" at cutover, and the Authorizing Official disagrees	Avalon uses the precise compliance statement in Section 5 and delivers evidence, not promises
Agency-side dependencies	SME time, account provisioning and test staffing slip, and the schedule slips with them	Each dependency is a dated government-furnished item with a named owner
Data migration as a footnote	Schema conversion and reconciliation take longer than the server move	Data migration is estimated and staffed as its own workstream
No one runs it afterward	Hypercare ends and the agency has no operations plan	Operations ownership is settled at the start; closeout includes a transition-to-O&M plan

Questions Agencies Ask

- **"Cloud ends up costing more than our data center."** It can, when everything is lifted and shifted with no dispositions and no governance. The assessment puts both cost paths side by side, including the refresh, licensing, facility and staffing costs the data center figure usually leaves out, before any wave is committed.
- **"We haven't worked with Avalon before."** That is why the entry point is a bounded, fixed-price assessment. The agency sees exactly how Avalon works before any migration dollar is obligated.
- **"Can a small firm handle our portfolio?"** Avalon states in writing how many waves it can staff at once and delivers them in sequence. If a portfolio needs a 60-person program, Avalon will say so.
- **"We tried this before and it stalled."** The assessment identifies what stopped the last attempt, whether disposition discipline, remediation capacity or agency-side bottlenecks, and the SOW assigns dates so it does not happen quietly again.
- **"Won't this lock us into one provider?"** Everything Avalon builds ships as infrastructure-as-code the agency owns, which is the practical form of exit readiness.

Where Migration Leads Next

A completed migration is a starting point. The work that follows is predictable, and planning for it early keeps the new environment from drifting back into the problems the migration solved.

Next step	Why it follows migration
FinOps and cost governance	Consumption begins at cutover; tagging, budgets and rightsizing keep the savings in the model from eroding
Enterprise Monitoring	Someone has to run and watch the environment after hypercare
DevSecOps and CI/CD	Refactored and replatformed applications now deploy as code
Zero Trust Architecture	The landing zone's identity, segmentation and logging are the base layers for zero trust milestones
SSP development and ATO facilitation	The evidence package from migration feeds the agency's system security plan and assessment directly

The calendar also matters. SEWP VI opens for orders on November 1, 2026. The AWS OneGov credits run through December 31, 2028. DoD's target-level zero trust deadline falls at the end of FY2027. Under FedRAMP's 2026 Consolidated Rules, solicitation and authorization language is moving to the new certification terminology. Each of these has a migration dependency built into it.

Conclusion and Next Step

Agencies do not need another modernization vision. They need their systems moved, on a schedule they can plan around, at a price they can defend, with the security evidence their assessors will ask for. Avalon delivers cloud migration as fixed-price waves led by senior engineers, with clear boundaries on what the work includes and an honest statement of how much Avalon can take on at once.

The first step is a fixed-price assessment and migration plan. It inventories and dispositions the portfolio, builds both cost paths from the agency's real numbers, names the government-furnished items that will decide the schedule, and prices each wave before any migration dollar is committed. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

ATO: Authority to Operate

The Authorizing Official's formal decision to accept the risk of operating a system, issued under the NIST Risk Management Framework.

CSP: Cloud Service Provider

A company that provides cloud infrastructure, platform or software services, such as AWS, Microsoft, Google or Oracle.

CUI: Controlled Unclassified Information

Government information that requires safeguarding under law, regulation or policy but is not classified.

FedRAMP

The federal program that standardizes security assessment of cloud products. Under its 2026 Consolidated Rules it certifies cloud offerings in lettered classes; agencies still authorize their own use.

FFP: Firm Fixed Price

A contract type where the price does not change with the contractor's actual cost.

IaC: Infrastructure-as-Code

Managing infrastructure through version-controlled configuration files rather than manual setup.

IL: Impact Level

DoD's categories for cloud data sensitivity under the Cloud Computing SRG: IL2 (public and low-sensitivity), IL4 (CUI), IL5 (higher-sensitivity CUI and national security systems) and IL6 (classified up to Secret).

Landing zone

The pre-configured cloud foundation (accounts, identity, network, logging and guardrails) that migrated workloads land in.

O&M: Operations and Maintenance

The recurring cost of running existing systems, and the one-year appropriation that usually funds it.

RMF: Risk Management Framework

The NIST SP 800-37 process agencies use to categorize, secure, assess, authorize and monitor systems.

SOW: Statement of Work

The contract document that defines scope, deliverables and government-furnished items.

Wave

A group of applications migrated together, planned by dependency, risk and mission calendar.

Appendix B: Compliance Mapping

The tables below show how migration activities support common control sets. They describe where the work produces evidence; they are not a statement that any system is compliant.

I. NIST SP 800-53 Rev. 5 (selected customer-responsibility controls)

Control	Name	How the migration supports it
AC-2	Account Management	Cloud accounts and roles federated to the agency identity provider and defined in code
AU-2 / AU-6	Event Logging; Audit Record Review	Centralized log architecture in the landing zone aligned to the agency's OMB M-26-14 logging plan
CM-2 / CM-6	Baseline Configuration; Configuration Settings	Configuration baselines captured as infrastructure-as-code and delivered to the agency
CP-9 / CP-10	System Backup; Recovery and Reconstitution	Backup and recovery configured and tested per wave, with rollback plans in each runbook
IA-2	Identification and Authentication	Application authentication moved to the agency's identity provider with MFA
SC-7	Boundary Protection	Network segmentation and controlled ingress and egress in the landing zone
SC-28	Protection of Information at Rest	Encryption baselines applied to storage and databases

II. ISO/IEC 27001:2022 (selected Annex A controls)

Annex A control	Name	How the migration supports it
A.5.9	Inventory of information and other associated assets	Portfolio inventory and dependency map delivered in the assessment
A.5.15	Access control	Role-based access defined in code and federated to the agency identity provider
A.5.23	Information security for use of cloud services	Shared-responsibility mapping using the provider's customer responsibility matrix
A.8.9	Configuration management	Version-controlled configuration baselines
A.8.15	Logging	Centralized logging built into the landing zone
A.8.32	Change management	Wave gates and the disposition change process

III. ISO 9001:2015 (quality management)

Clause	Requirement	How the migration supports it
8.1	Operational planning and control	Wave plan, runbooks and written acceptance criteria
8.5.1	Control of production and service provision	Rehearsed cutovers with defined validation steps
9.1	Monitoring, measurement, analysis and evaluation	Per-wave acceptance results and hypercare issue tracking
10.2	Nonconformity and corrective action	Pilot-wave lessons applied to production wave estimates and runbooks

Appendix C: Cost-Model Assumptions

All values are Avalon planning assumptions for a representative portfolio, in constant FY2026 dollars. None is drawn from a specific agency or a completed engagement.

Category	Assumption	Basis
Portfolio	30 applications: retire 4, repurchase 3, rehost 12, replatform 8, refactor 2, retain 1	Representative mid-size unclassified portfolio
Legacy run cost	Sustainment labor (10 FTE): \$1,650K per year	Avalon planning assumption
Legacy run cost	Data center hosting, power and space: \$600K per year	Avalon planning assumption
Legacy run cost	Hardware maintenance contracts: \$250K per year	Avalon planning assumption
Legacy run cost	Virtualization, OS and database licensing: \$900K per year	Avalon planning assumption
Legacy refresh	Hardware refresh of \$2.40M due in Year 1 (status quo only)	The trigger event in this example

Category	Assumption	Basis
Target run cost	Sustainment labor (6 FTE): \$990K per year from Year 2	Avalon planning assumption
Target run cost	Cloud consumption, 22 migrated apps (rightsized): \$1,100K per year from Year 2	Avalon planning assumption
Target run cost	SaaS subscriptions, 3 repurchased apps: \$150K per year from Year 2	Avalon planning assumption
Target run cost	Residual hosting, 1 retained app: \$120K per year from Year 2	Avalon planning assumption
Target run cost	Remaining licensing (managed DB, BYOL): \$350K per year from Year 2	Avalon planning assumption
Target run cost	Monitoring and cost-governance tooling: \$80K per year from Year 2	Avalon planning assumption
Agency program cost (Year 1)	Agency PMO, ISSO and UAT time: \$300K	Avalon planning assumption
Agency program cost (Year 1)	Reassessment of the new boundary (assessor): \$250K	Avalon planning assumption
Agency program cost (Year 1)	Legacy decommissioning and data sanitization: \$100K	Avalon planning assumption
Agency program cost (Year 1)	Maintenance bridge on legacy hardware (no refresh): \$150K	Avalon planning assumption
Labor rate	\$165K fully loaded per sustainment FTE per year	Avalon planning assumption
Dual running	75% of legacy run cost and 50% of cloud and SaaS run cost incurred in Year 1	Waves cut over through the year

Category	Assumption	Basis
Avalon services	Per-application rates inside the market bands in Section 6	Rehost \$40K, replatform \$95K, refactor \$250K (T&M ceiling)
Discount rate	1.3% real, mid-year convention	OMB Circular A-94 Appendix C, 5-year real rate for 2026
Excluded	Cloud provider credits (shown only as a sensitivity), inflation, facility exit costs	Kept out to avoid overstating the case

Appendix D: References

1. **U.S. Government Accountability Office**, *Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems* (GAO-25-107795), July 2025
<https://www.gao.gov/products/gao-25-107795>
2. **Office of Management and Budget**, *Circular A-94, Appendix C: Discount Rates for Cost-Effectiveness Analysis* (2026)
<https://www.whitehouse.gov/wp-content/uploads/2026/03/CircularA-94Appendix-C.pdf>
3. **U.S. General Services Administration**, *GSA Announces OneGov Agreement with AWS*, August 7, 2025
<https://www.gsa.gov/about-us/newsroom/news-releases/gsa-announces-onegov-agreement-with-aws-08072025>
4. **FedRAMP**, *FedRAMP Consolidated Rules for 2026: Definitions*
<https://www.fedramp.gov/2026/definitions/>
5. **NASA SEWP**, *SEWP VI Transition Updates*
https://www.sewp.nasa.gov/sewpv/sewpvi_transition_updates.shtml
6. **The White House**, *Executive Order 14028, Improving the Nation's Cybersecurity* (May 2021), as amended by *Executive Order 14306* (June 2025)
<https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

7. **Office of Management and Budget**, *M-26-14, Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats (May 2026)*
<https://www.whitehouse.gov/wp-content/uploads/2026/05/M-26-14-Ensuring-Effective-and-Efficient-Agency-Logging-and-Network-Visibility-to-Defend-Against-Evolving-Cyber-Threats.pdf>
8. **Office of Management and Budget**, *M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 2022)*
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
9. **U.S. Department of Defense**, *DoD Zero Trust Strategy (November 2022)*
<https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
10. **NIST**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
11. **NIST**, *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>
12. **NIST**, *SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>
13. **DISA**, *Department of Defense Cloud Computing Security Requirements Guide*
<https://public.cyber.mil/dccs/>