



Securing Tomorrow's Missions Today.



## **Build the Foundation Once: Cloud Architecture & Engineering for Federal Programs**

---

Cloud Architecture & Engineering: landing zones built as code, mapped to NIST SP 800-53, and documented for the agency's own authorization.

|                                                        |           |
|--------------------------------------------------------|-----------|
| <b>Executive Summary</b>                               | <b>2</b>  |
| <b>Why Federal Cloud Environments Stall</b>            | <b>2</b>  |
| Why It Concentrates in Government                      | 3         |
| How the Need Sounds                                    | 3         |
| <b>What Is Changing in 2026 and 2027</b>               | <b>4</b>  |
| <b>What an Engineered Landing Zone Contains</b>        | <b>4</b>  |
| Built as Code, Owned by the Agency                     | 5         |
| <b>Evidence as You Build</b>                           | <b>6</b>  |
| Where the Work Sits in the RMF                         | 7         |
| Saying It Accurately                                   | 8         |
| <b>How an Engagement Runs</b>                          | <b>9</b>  |
| What the Agency Provides                               | 9         |
| What Is Not Included                                   | 10        |
| <b>Scope Avalon Takes On Today</b>                     | <b>10</b> |
| <b>Pricing and How to Buy</b>                          | <b>11</b> |
| <b>Illustration: When Does a Landing Zone Pay Off?</b> | <b>12</b> |
| Lead Time Matters More Than Cost                       | 13        |
| <b>Common Pitfalls</b>                                 | <b>13</b> |
| <b>Conclusion and Next Step</b>                        | <b>13</b> |
| <b>Appendices</b>                                      | <b>14</b> |
| Appendix A: Glossary                                   | 14        |
| Appendix B: Illustration Assumptions                   | 15        |
| Appendix C: References                                 | 16        |

## Executive Summary

Most federal agencies now have cloud contracts, modernization mandates and discounted consumption. What many do not have is a secure foundation to put systems on. Each new program stands up its own environment, one workload at a time: its own accounts, network, logging and guardrails, built by whoever was available. Programs wait months for an environment the ISSM will accept, security reviews stall on boundaries nobody designed, and the bill grows with every duplicate.

Cloud Architecture & Engineering is the work that fixes this at the root. It designs the agency's target cloud environment, builds it as infrastructure-as-code, maps its guardrails to NIST SP 800-53 controls, and delivers the evidence the agency's security team needs to carry it through authorization. New programs then receive a compliant environment from the platform in weeks, instead of building one from scratch.

This paper is written for CIOs and cloud program offices, CISOs and ISSMs, the program managers waiting on environments, and the contracting officers who buy the work. It describes Avalon Technology Services' service in two shapes:

- **An architecture assessment and target-state blueprint.** A fixed-price, design-only engagement of 6 to 9 weeks, priced well under the simplified acquisition threshold.
- **A landing zone design and build.** A milestone-based fixed-price engagement of about 3.5 to 6 months that delivers the environment as code, with environment vending and control-implementation evidence.

Section 9 works through an illustrative agency with eight new programs over three years. Building each program its own environment costs about \$1.70M in engineering labor; one landing zone plus vended environments costs about \$1.03M. The landing zone pays for itself at the fifth program, and after the build each new program waits about 3 weeks for an environment instead of 24. With only three programs, it does not pay off, and the paper says so.

Final authorization always stays with the agency's Authorizing Official. Avalon builds to the standard and documents it; the government makes the decision.

## Why Federal Cloud Environments Stall

The problem is rarely the cloud provider. It is the agency's side of the shared responsibility line, the layer each program is left to build on its own.

| Risk             | How it shows up                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mission risk     | Programs sit in a queue because no compliant environment exists to deploy into. Every month without an environment is a month without the capability.                                       |
| Compliance risk  | Ad hoc environments produce authorization boundaries no ISSM can defend and control implementations no assessor can verify. Reviews stall, or pass with conditions that become POA&M items. |
| Cost risk        | Duplicated environments, unmanaged accounts, missing tags and absent guardrails. Sprawl is an architecture failure before it is a financial one.                                            |
| Operational risk | Hand-built environments cannot be rebuilt after an incident, cannot be copied for the next program, and depend on the memory of whoever configured the console.                             |

## Why It Concentrates in Government

- **Mandate timing.** FISMA, RMF, FedRAMP, DoD impact levels, zero trust and TIC 3.0 all constrain how an environment must be built, and agencies often sign cloud contracts before anyone has designed one that satisfies them.
- **Staffing gaps.** Cloud architecture and platform engineering are among the hardest federal positions to fill and keep. Programs inherit environments built by whoever was on hand.
- **Budget shape.** Consumption dollars are easy to obligate. Engineering dollars to build the foundation often are not, so agencies end up with funded cloud contracts and unfunded foundations.
- **Legacy pressure.** Data-center exits and expiring leases force timelines that outrun architecture. "Lift and shift now, fix it later" becomes the default.

## How the Need Sounds

"Every program stands up its own environment." "It takes six months to get a new system an environment." "Security keeps rejecting our boundary." "We lifted and shifted, and it costs more than the data center did." "We have the cloud contract, but nothing

has moved." "Our cloud engineer left and nobody knows how it's set up." Each of these is a foundation problem, not an application problem.

## What Is Changing in 2026 and 2027

| Driver                                               | What it means for the foundation                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FedRAMP Consolidated Rules (published June 25, 2026) | Cloud offerings are now "FedRAMP Certified" in classes A through D, and the program is moving to continuous, machine-readable evidence. New Rev5 submissions stop June 11, 2027, and Rev5 authorizations end December 31, 2028. Certification still covers only the provider's offering; the agency authorizes its own systems. |
| Zero trust deadlines                                 | OMB M-22-09 set the civilian zero trust strategy, and DoD's zero trust strategy targets its target-level capabilities by the end of FY2027. Identity, segmentation and visibility are largely built in the cloud environment layer.                                                                                             |
| TIC 3.0                                              | Boundary and telemetry design follows CISA's cloud use cases rather than routing everything through a physical access point.                                                                                                                                                                                                    |
| GSA OneGov agreements                                | Discounted consumption from the major providers, including up to \$1 billion in AWS incentive credits through December 31, 2028, lowers the cost of using cloud without lowering the cost of engineering it well.                                                                                                               |
| AI workloads                                         | New AI initiatives need data-governed, GPU-capable environments that most agencies cannot stand up program by program.                                                                                                                                                                                                          |

The direction is the same in each case: environments defined as code, with control mappings and evidence produced as the environment is built. That is what this service delivers.

## What an Engineered Landing Zone Contains

A landing zone is the secure neighborhood the agency's systems live in. It is built once, correctly, and documented so the agency can prove it is correct.

| Layer | What is designed and built |
|-------|----------------------------|
|-------|----------------------------|

|                                    |                                                                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account and subscription structure | Organizational units or management groups by mission, environment and impact level; separate accounts for logging, security tooling and shared services                          |
| Network and boundary               | Hub-and-spoke or transit topology, segmentation, hybrid connectivity (Direct Connect or ExpressRoute), and boundary protection aligned to TIC 3.0 or DoD connection requirements |
| Identity                           | Federation to the agency's enterprise ICAM, role design, privileged access patterns and break-glass procedures                                                                   |
| Logging and monitoring             | Centralized, tamper-resistant log collection and the telemetry plumbing a security operations team needs                                                                         |
| Encryption and keys                | At-rest and in-transit encryption standards, key management design and key ownership                                                                                             |
| Guardrails                         | Policy-as-code (service control policies, Azure Policy, AWS Config rules, Open Policy Agent), each mapped to the NIST SP 800-53 control it implements                            |
| Baselines                          | CIS Benchmarks or DISA STIGs applied to images and services, verified by automated scanning                                                                                      |
| Backup and contingency             | Backup architecture and recovery design that support CP-9 and CP-10                                                                                                              |
| Environment vending                | A repeatable way to issue a new program a compliant environment on request, already inside the guardrails                                                                        |

Every significant choice is captured in an architecture decision record, so the agency knows not just what was decided but why. The first workload enclave is built end to end to prove the pattern before any program depends on it.

## Built as Code, Owned by the Agency

The environment is delivered as Terraform, CloudFormation or Bicep in the agency's own repository, with data rights set by the contract. It can be reviewed line by line, rebuilt after an incident, and copied for the next program. Build tooling includes AWS Control Tower and the Landing Zone Accelerator, the Azure landing zone reference implementations, and the major providers' architecture frameworks. Validation uses open-source scanners such as Prowler, ScoutSuite and Checkov against the agency's chosen baseline. No new licensed platform is required, and none is sold.

## Evidence as You Build

The difference between an environment and an authorizable one is evidence. This service produces control-implementation statements, boundary and data-flow diagrams, and inherited-versus-agency-implemented control documentation as the environment is built, in a form the agency's ISSO can drop into the SSP.

| Control family                  | What the environment implements and documents                          |
|---------------------------------|------------------------------------------------------------------------|
| AC                              | Access enforcement through role design and guardrails                  |
| AU-2, AU-6, AU-12               | Logging architecture, central collection and review support            |
| CM-2, CM-6, CM-7                | Baseline configurations, hardened settings and least functionality     |
| CP-9, CP-10                     | Backup and recovery design                                             |
| IA-2, IA-5                      | Identity federation and authenticator management                       |
| SC-7, SC-8, SC-12, SC-13, SC-28 | Boundary protection, encryption in transit and at rest, key management |
| SI-4                            | Monitoring plumbing for the agency's security operations               |

## Where the Work Sits in the RMF

| RMF step (SP 800-37 Rev. 2) | This service                                           | Who owns it                            |
|-----------------------------|--------------------------------------------------------|----------------------------------------|
| Prepare                     | Architecture inputs, boundary definition               | Agency, supported                      |
| Categorize                  | Impact-level and baseline mapping inputs               | System owner                           |
| Select                      | Control tailoring inputs and inheritance documentation | System owner and ISSM                  |
| Implement                   | Builds and documents the environment-layer controls    | This service                           |
| Assess                      | Provides evidence; does not assess                     | An assessor independent of the builder |
| Authorize                   | None                                                   | The Authorizing Official               |
| Monitor                     | Monitoring architecture only                           | Agency continuous monitoring program   |

Avalon does not assess or authorize what Avalon builds. Keeping the builder and the assessor separate protects the agency's authorization, and Avalon states it in every proposal as an organizational conflict-of-interest position.

## Saying It Accurately

| Accurate                                                                                                                                  | Not accurate                    |
|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| Designed and implemented to the NIST SP 800-53 Rev. 5 moderate baseline, with control-implementation evidence for the agency's assessment | An 800-53-compliant environment |
| An authorization-ready environment with SSP-ready boundary and data-flow documentation                                                    | ATO guaranteed                  |
| Deployed on FedRAMP Certified cloud services at the appropriate class, with documented control inheritance                                | A FedRAMP Certified environment |
| Engineered to DoD Cloud Computing SRG IL4 requirements                                                                                    | IL4 authorized                  |

## How an Engagement Runs

| Phase                              | Typical duration | What happens                                                                                                                                 |
|------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 0. Kickoff and access              | 1–2 weeks        | Stakeholder alignment, read-only access for discovery, agency security review of the toolset                                                 |
| 1. Discovery                       | 2–4 weeks        | Inventory of accounts and tenants, interviews with system owners and the ISSM, posture review, cost and tagging snapshot, document review    |
| 2. Target architecture             | 3–5 weeks        | Account model, network, identity, logging and guardrail design; design reviews with the ISSM and AO representatives; decision records        |
| 3. Landing zone build              | 4–10 weeks       | Infrastructure-as-code, guardrails, shared services, environment vending and a first workload enclave; demonstrations every one to two weeks |
| 4. Validation and documentation    | 2–3 weeks        | Compliance scans, control-implementation evidence, boundary and data-flow documentation, runbooks                                            |
| 5. Knowledge transfer and closeout | 1–2 weeks        | Working sessions with agency engineers and security staff; backlog handoff                                                                   |

A design-only engagement covers phases 0 through 2 plus documentation and runs 6 to 9 weeks. A full design and build runs about 3.5 to 6 months. Each added impact level, enclave, cloud provider or new connectivity path moves the schedule toward the long end.

## What the Agency Provides

- An executive sponsor who can make architecture decisions, with a five-business-day turnaround on escalated items. Items undecided after ten business days trigger schedule relief attributable to the government.

- System owner and ISSM or ISSO time, roughly two to four hours a week, with design reviews treated as mandatory.
- Network and identity team participation. Connection approvals and new circuits are often the longest lead-time items in the schedule.
- Tenant and account provisioning authority and funded cloud consumption. Consumption is the agency's cost and is never inside the engagement price.
- Existing documentation: network diagrams, inventories, SSPs, POA&Ms and prior assessments where they exist.
- Security review of the delivery toolset before discovery begins.

## What Is Not Included

| Included                                                       | Separate work                                                                                      |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Environment and landing zone design and build                  | Moving or refactoring applications (Cloud Migration & Development)                                 |
| Control-implementation evidence and architecture documentation | The complete SSP package and running the authorization (SSP and ATO Process Facilitation services) |
| Logging and monitoring architecture                            | Ongoing monitoring operations and alert triage (Enterprise Monitoring)                             |
| Cost-aware design: tagging, budgets, account strategy          | Spend recovery and forensic cost audit (FinOps)                                                    |
| A testable, assessable environment                             | Testing it, which is performed independently of the builder                                        |

## Scope Avalon Takes On Today

Avalon takes one design-and-build engagement at a time, led by its founder. The assessment and blueprint can run alongside it. Scope is stated plainly so the agency can plan around it:

| Environment                                                                                     | Position                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unclassified civilian workloads up to the FedRAMP Class C (formerly Moderate) baseline; DoD IL2 | In scope                                                                                                                                                                                   |
| DoD IL4                                                                                         | In scope, single enclave                                                                                                                                                                   |
| DoD IL5                                                                                         | Only where the agency's personnel requirements can be met. Where cleared personnel are required, cleared staff are a named condition of the engagement, provided through a teaming partner |
| IL6, classified and Intelligence Community environments                                         | Out of scope                                                                                                                                                                               |
| Enterprise-wide, multi-enclave programs                                                         | As the architecture cell within a larger team                                                                                                                                              |

Named key personnel and their credentials are listed in each proposal. Avalon cites no credential, clearance or past engagement that is not current and verifiable, and it has no prior federal contracts under this service.

## Pricing and How to Buy

| Engagement                                                | Typical scope                           | Market-norm range                         |
|-----------------------------------------------------------|-----------------------------------------|-------------------------------------------|
| Assessment and target-state blueprint                     | 4–8 weeks, one environment, design only | \$60K–\$150K FFP<br>(Avalon: \$65K–\$95K) |
| Landing zone design and build, unclassified, one provider | 3–5 months, civilian or IL2             | \$250K–\$600K FFP                         |
| IL4/IL5, multi-enclave or multi-cloud build               | 4–8 months                              | \$500K–\$1.5M                             |
| Architecture health check                                 | 2–3 weeks                               | \$25K–\$60K                               |

Builds are priced as milestone-based fixed price, so the agency pays for accepted deliverables. Pricing is never tied to an authorization outcome, because that outcome belongs to the government.

The blueprint fits under the \$350,000 simplified acquisition threshold, so it can be bought as an open-market purchase with simplified procedures and one-year O&M funds. Larger builds can be bought the same way when they are scoped under the threshold, or through a prime that already holds the agency's vehicle, with Avalon as a subcontractor. Avalon does not hold a GSA Schedule or a governmentwide contract today.

## Illustration: When Does a Landing Zone Pay Off?

The figures below are a planning illustration for one agency cloud program office, not a quote and not a result from any engagement. They count engineering labor only. Cloud consumption is excluded because the agency pays it under either path.

The office expects eight new programs over three years, arriving evenly. Under the bespoke path, each program gets its own hand-built environment: about \$140K of engineering, \$35K of rework when the assessor finds boundary or evidence gaps, 24 weeks from request to an environment the ISSM accepts, and \$30K a year to keep its own logging, network and guardrails current. Under the landing zone path, the office buys an \$80K blueprint and a \$420K build that take about 22 weeks, then vends each program an environment for \$25K in 3 weeks, with \$8K a year of per-program upkeep and \$90K a year to run the platform.

| Scenario                                           | Bespoke, 3 years | Landing zone, 3 years | Difference |
|----------------------------------------------------|------------------|-----------------------|------------|
| Base case (8 programs in 3 years)                  | \$1.70M          | \$1.03M               | \$664K     |
| Fewer programs (3 in 3 years)                      | \$663K           | \$850K                | (\$187K)   |
| Build at top of band (\$600K)                      | \$1.70M          | \$1.21M               | \$484K     |
| Slow agency decisions (landing zone 10 weeks late) | \$1.70M          | \$1.09M               | \$605K     |

*Parentheses mean the landing zone path costs more. Discounting at the 2026 OMB Circular A-94 three-year real rate of 1.1% changes no total by more than about 2%.*

In the base case, the landing zone path costs about \$664K less over three years, and it starts costing less than the bespoke path at the fifth program. A build at the top of the

price band moves that to the sixth program. With only three programs, the bespoke path is cheaper by about \$187K; an office in that position is better served by the blueprint alone, applied program by program.

## Lead Time Matters More Than Cost

The larger effect is on schedule. Under the bespoke path, every program waits about 24 weeks. Under the landing zone path, the first program waits for the build, about 25 weeks, and the second about 6; every later program waits 3. If agency decisions slow the build by ten weeks, the first program waits about 35 weeks and the second about 16, while the cost advantage barely moves. That is why the decision turnaround clause sits in the statement of work: the agency's own decision speed sets how soon the first programs benefit.

## Common Pitfalls

| Pitfall                                           | How to avoid it                                                                                              |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Application migration creeping into the build     | Workload migration is separately priced work; the statement of work says so                                  |
| "Just one more environment"                       | Enumerate the environments and impact levels in scope, with a count cap; additions go through a change order |
| An operations tail forming after the build        | Define done as milestone acceptance; sustainment is a separate decision                                      |
| Agency-side delays becoming the vendor's schedule | Name each government dependency with a needed-by date and a decision turnaround clause                       |
| Compliance overselling                            | Use the accurate language in Section 5 in the proposal, the statement of work and every status report        |

## Conclusion and Next Step

Agencies that build cloud environments one program at a time pay for the same foundation again and again, and wait for it every time. An engineered landing zone, delivered as code with its evidence, turns that into a platform that issues compliant environments in weeks and gives the ISSM a boundary that can be defended.

The natural first step is the architecture assessment and target-state blueprint: one environment, design only, a fixed price under the simplified acquisition threshold, and a clear recommendation on whether a full landing zone is worth building for the agency's pipeline of programs. To discuss a blueprint, contact Avalon Technology Services at [contact@AvalonTechServices.com](mailto:contact@AvalonTechServices.com).

## Appendices

### Appendix A: Glossary

**AO: Authorizing Official**

The senior official who accepts the risk of operating a system and grants the authorization to operate.

**ICAM**

Identity, Credential and Access Management: the agency's enterprise identity program.

**IL: Impact Level**

The DoD Cloud Computing SRG category (IL2, IL4, IL5, IL6) that sets requirements by data sensitivity.

**Infrastructure-as-code (IaC)**

Defining an environment in version-controlled configuration files that can be reviewed, rebuilt and copied.

**Landing zone**

The engineered foundation of accounts, network, identity, logging and guardrails that workloads are deployed into.

**Policy-as-code**

Guardrails written as machine-enforced rules, such as service control policies or Azure Policy.

**RMF**

The NIST Risk Management Framework, SP 800-37 Rev. 2: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor.

**TIC 3.0**

CISA's Trusted Internet Connections guidance for securing agency network traffic, including cloud use cases.

**Vending**

Issuing a new program a pre-configured, compliant environment from the landing zone on request.

## Appendix B: Illustration Assumptions

All values are planning assumptions for one representative agency cloud program office. None is drawn from a specific agency or a completed engagement.

| Assumption                      | Value                                                        | Basis                                               |
|---------------------------------|--------------------------------------------------------------|-----------------------------------------------------|
| Horizon and programs            | 3 years; 8 programs, evenly spaced (3 in the alternate case) | Planning assumption                                 |
| Bespoke environment engineering | \$140K per program                                           | About 900 hours at a \$155 blended rate             |
| Assessment rework, bespoke      | \$35K per program                                            | Planning assumption                                 |
| Bespoke lead time               | 24 weeks                                                     | Request to an environment the ISSM accepts          |
| Bespoke upkeep                  | \$30K per environment per year                               | Planning assumption                                 |
| Blueprint and build             | \$80K and \$420K (\$600K alternate)                          | Inside the market-norm bands in Section 8           |
| Build duration                  | 22 weeks (32 with slow decisions)                            | Within the 3.5–6 month range                        |
| Delay cost                      | \$8K per week of agency-attributable delay                   | Change order for a reduced team on standby          |
| Vending                         | \$25K and 3 weeks per program                                | Planning assumption                                 |
| Platform and per-program upkeep | \$90K a year; \$8K per program a year                        | Planning assumption                                 |
| Discount rate                   | 1.1% real                                                    | OMB Circular A-94 Appendix C, 2026, three-year rate |
| Excluded                        | Cloud consumption, application migration, authorization      | Outside the comparison                              |

## Appendix C: References

1. **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>
2. **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>
3. **National Institute of Standards and Technology**, *SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems*  
<https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final>
4. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*  
<https://www.fedramp.gov>
5. **Crowell & Moring**, *Time for a Change: FedRAMP Fundamentally Revamps Program With Consolidated Rules for 2026*, July 7, 2026  
<https://www.crowell.com/en/insights/client-alerts/time-for-a-change-fedramp-fundamentally-revamps-program-with-consolidated-rules-for-2026>
6. **Defense Information Systems Agency**, *DoD Cloud Computing Security Requirements Guide*  
<https://public.cyber.mil/dccs/>
7. **Office of Management and Budget**, *M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022  
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
8. **DoD Chief Information Officer**, *DoD Zero Trust Strategy*  
<https://dodcio.defense.gov/Library/>
9. **Cybersecurity and Infrastructure Security Agency**, *Trusted Internet Connections 3.0*  
<https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic>
10. **Cybersecurity and Infrastructure Security Agency**, *Zero Trust Maturity Model, Version 2.0*  
<https://www.cisa.gov/zero-trust-maturity-model>
11. **Amazon Web Services**, *AWS Well-Architected Framework*  
<https://aws.amazon.com/architecture/well-architected/>

12. **Microsoft**, *Cloud Adoption Framework: Azure landing zones*  
<https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/>
13. **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/>