



Securing Tomorrow's Missions Today.



Your Default Environment Is Already an App Portfolio: A Fixed-Fee Power Platform Governance and App Triage for Agency CIOs and ISSMs

Low Code / No Code: environment strategy, data loss prevention and an inventory-backed triage of the apps your makers already built, on the platform you already license

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
How a Licensed Platform Becomes Shadow IT	3
What Goes Wrong Without Governance	3
The Drivers and the Calendar	5
What the Engagement Does	7
The App Disposition	8
Deliverables	9
Where the Engagement Stops	9
Evidence the ISSM Can Use	10
How an Engagement Runs	11
What the Agency Provides	11
What Is Not Included	12
How Avalon Staffs It	12
Pricing and How to Buy	13
Illustration: One Tenant, Ten Weeks	14
The Governance Gap	14
Dispositions and the Rebuild Backlog	15
What the Engagement Costs	16
Common Pitfalls	17
Conclusion and Next Step	17
Appendices	18
Appendix A: Glossary	18
Appendix B: Illustration Assumptions	18
Appendix C: References	19

Executive Summary

Most agencies that run Microsoft 365 already have a low-code platform, and most of them already have a low-code portfolio they never planned. Power Apps and Power Automate come with the license. Staff build trackers, intake forms and approval flows to get work done, and nearly all of it lands in the default environment, where every licensed user can build and the connector rules are whatever they were on day one. Nobody counted it, nobody owns half of it, and the security team finds out when an app touching personal data turns up in a data call.

Two Microsoft announcements turned that quiet sprawl into a deadline. Microsoft retired SharePoint 2013 workflows in SharePoint Online on April 2, 2026, and announced end of support for InfoPath 2013 on July 14, 2026. Offices that ran approvals and forms on those tools now have broken processes, and the replacement they are pointed to is the Power Platform they already license.

This paper is for the people who own that platform and its risk: the CIO's applications or business-systems chief and the platform owner who fund it, the ISSM or ISSO who carries the finding, the program office director whose process broke, and the COR who buys the work. It describes Avalon Technology Services' Low Code / No Code service, which starts with one engagement:

- **A fixed-fee Power Platform governance and app triage.** About ten weeks in the agency's own tenant. Environment strategy by data type, data loss prevention (DLP) and connector policy, managed environments, an inventory of every app and flow using Microsoft's Center of Excellence (CoE) Starter Kit, application lifecycle management (ALM) standards, a licensing posture review and a governance playbook, plus a disposition for every existing app and dead legacy form. The market band for this work is \$50K to \$150K firm fixed price.
- **A smaller entry option.** A legacy form and workflow triage of about four weeks, in the \$15K to \$35K band, that produces a prioritized, priced rebuild backlog.
- **Conditional follow-on builds.** Each rebuild in the backlog is a separately priced, fixed-fee application build, typically \$25K to \$150K, most of them well under the simplified acquisition threshold.

Section 9 works through an illustrative tenant with 230 apps and 540 flows. The base engagement is 520 hours over ten weeks: \$70.0K to \$103.6K, with a \$87K planning fee, well under the \$350,000 simplified acquisition threshold.

The service configures the platform and evidences the configuration. The authorization decision remains the government's. Avalon does not issue or guarantee an ATO, does

not certify Section 508 conformance, and never acts as the independent assessor of work it delivered.

How a Licensed Platform Becomes Shadow IT

The platform is not the problem. Federal case management, grants intake and inspection workflows run on low-code platforms today, inside certified government clouds. The problem is that an included license arrives without an environment strategy, and makers fill the gap. The phrases below come up in almost every first conversation.

What the office says	What it usually means
"We track that in a spreadsheet on the shared drive."	A process with no system of record, and no audit trail
"Our InfoPath forms stopped working."	A legacy estate nobody has counted, with no rebuild plan
"Only one person knows how that Access database works."	A single point of failure about to retire
"We're paying for G5 and basically using it for email."	Entitlements already bought, with no governed way to use them
"People built a bunch of Power Apps on their own and now security is involved."	A default environment full of apps with unknown owners, connectors and data

Two or more of those in one conversation usually means the office is asking for one app when the real need is governance first.

What Goes Wrong Without Governance

- **Everything lands in the default environment.** Every licensed user can build there, so business apps, personal tools and experiments share one space and one set of connector rules.
- **Connectors mix business and personal data.** Without a DLP policy, one flow can read a SharePoint list of case data and post it to a consumer service.
- **Owners leave and apps stay.** An app built by someone who has transferred keeps running under nobody's account until it breaks or leaks.

- **Premium licensing shows up after deployment.** A premium connector or Dataverse capacity requirement becomes a surprise bill instead of a design input.
- **Personal-grade apps become enterprise systems.** No ALM, no test evidence, no support model, and no record in the system security plan.

The Drivers and the Calendar

Driver	What it says	What it means for this engagement
Microsoft announcements on legacy forms and workflows	SharePoint 2013 workflows retired in SharePoint Online on April 2, 2026; InfoPath 2013 end of support on July 14, 2026	The database trigger; the triage counts every dead form and workflow and gives each a disposition
FedRAMP Consolidated Rules (Jun 25, 2026)	Cloud offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	The platform is certified; the agency configures its apps and authorizes its own systems
NIST SP 800-53 Rev. 5	App-level controls remain the agency's: AC-2, AC-3, AC-6, AU-2, AU-12, CM-3, CM-5, AT-2, AT-3	Role design, audit settings, ALM change control and maker training are configured and evidenced
NIST SP 800-37 Rev. 2	Seven RMF steps, starting with Prepare; changes are tracked against the authorized boundary	Most apps are a documented change inside an existing boundary; the ISSO decides
Section 508 and the 21st Century IDEA Act (2018)	The 2017 refresh incorporates WCAG 2.0 AA; WCAG 2.1 and 2.2 are current W3C guidance	Apps are ICT; builds are tested to 2.0 AA and to 2.1/2.2 as guidance, and reports say which
OMB M-25-21 (April 2025)	Governance of federal AI use; replaced M-24-10	Applies only where an app uses AI features such as Copilot Studio or document extraction
Privacy Act and NARA records requirements	PII may trigger a privacy impact assessment or a system of records notice; apps can become recordkeeping systems	The inventory flags PII and records candidates for the privacy and records officers

Driver	What it says	What it means for this engagement
OMB M-26-05 (Jan 23, 2026)	Rescinded M-22-18 and M-23-16; agencies set risk-based software assurance policy	SSDF is guidance and an SBOM is a contract term the agency may choose, not a mandate

Flows and bots that act on their own need their own identities. A flow that runs under a departed employee's account, or under a shared administrator login, fails the intent of IA-2, AC-2 and AC-6. The governance design moves automated work to service accounts or service principals with least privilege.

What the Engagement Does

The engagement covers one Microsoft Power Platform tenant that the agency already licenses, unclassified, in the commercial or GCC cloud first, with GCC High as a condition of named staff experience. It configures inside the agency's tenant with access the agency provisions, and installs nothing of Avalon's. Standing up a tenant from nothing is Avalon's separate SaaS/IaaS Implementation service; this engagement starts with a tenant that exists and makers who are already building.

Workstream	Activities
Inventory	Deploy the CoE Starter Kit; inventory every environment, app, flow, connector and maker; tag owner status, connector mix, data sensitivity and last use
Environment strategy	Default versus dedicated environments; placement by data type; GCC versus GCC High where CUI is involved
DLP and connector policy	Business, non-business and blocked connector groups for the default environment and each dedicated environment
Managed environments	Sharing limits, usage insights, maker welcome content and solution checker enforcement
ALM standards	Solution structure, pipelines, source control, release gates and the promotion path from personal to managed
Licensing posture	Map planned workloads to entitlements already held: seeded rights, premium connectors, Dataverse capacity, per-app versus per-user
Triage	A disposition for every existing app and every dead InfoPath form or SharePoint 2013 workflow, and a priced rebuild backlog
Governance playbook	The operating document the agency's platform team runs after handoff

The App Disposition

Every app and legacy item ends in one of five dispositions: retire (after the records officer confirms retention), leave personal under default-environment DLP, promote to a managed environment, rebuild as a governed build, or route to another service. Each disposition rests on recorded evidence: last use, owner status, connectors, data sensitivity and how many people depend on it. The rule for the last category is simple: if the requirement can be met with platform-native components plus configuration, it is low code. Sustained custom code, or orchestration across many systems, belongs to a different service.

Deliverables

Deliverable	Format
Inventory and disposition workbook: every app, flow and legacy item, tagged	XLSX, refreshed from the CoE Starter Kit
Environment strategy and placement rationale	Document with diagrams, written to drop into the ISSO's documentation
DLP and environment configuration	Applied in the tenant, plus exported policy documentation
ALM pipeline and runbook	Configured pipeline with a written runbook
Licensing posture review	Seat and capacity counts; dollar values only from agency-entered unit prices
Priced rebuild backlog	One line per build, tiered and banded, with SAT fit flagged
Governance playbook	Operating document for the platform team

Where the Engagement Stops

The engagement does not resell licenses, provision a tenant, write the system security plan or drive the ATO package. Those are separate Avalon services: SaaS/IaaS Implementation, System & Application Security Plans and ATO Process Facilitation. Enterprise robotic process automation belongs to Process Automation; custom-coded replacements belong to Application Modernization or Cloud Native Development. Appian, ServiceNow and Salesforce are not offered as the lead platform today, and Avalon does no classified work.

Evidence the ISSM Can Use

The platform's FedRAMP certification covers the provider's offering. Inheritance from it is partial and is the Authorizing Official's call. What remains is the agency's app-level configuration, and that is what this engagement configures and documents.

Control	What the engagement configures and evidences
AC-2, AC-3, AC-6	Environment security roles, sharing limits, least-privilege service accounts for flows
IA-2	Automated work runs under its own identities, not a person's account
AU-2, AU-12	Audit settings enabled and documented per environment
CM-3, CM-5	ALM pipeline, solution packaging and release gates as change control
CM-8	An inventory of apps, flows and connectors the SSP can cite
AT-2, AT-3	Maker guidance and role-based training content in the playbook

The accurate way to say it: Avalon configures the platform within the agency's tenant to the platform's certified baseline, and delivers the security design, role matrix and configuration evidence in a format that supports the ISSO's change and authorization documentation.

Accurate	Not accurate
Configures DLP and environments to the certified baseline	Makes the apps FedRAMP compliant
Delivers an inventory and configuration evidence	The apps inherit the ATO
Documents accessibility test results for builds	Certifies Section 508 conformance
An input to the ISSO, the assessor and the AO	Guarantees an assessment outcome

How an Engagement Runs

Phase	Timing	What happens
0: Kickoff and access	1–2 weeks, in parallel	Tenant admin roles, accounts, PIV where required; dependencies dated in writing
1: Inventory	2–3 weeks	CoE Starter Kit deployed; inventory tagged; ISSO confirms placement rules
2: Design and configuration	4–5 weeks	Environment strategy, DLP, managed environments, ALM pipeline, licensing posture
3: Triage and playbook	2–3 weeks	Dispositions, priced rebuild backlog, governance playbook, readout
Builds (separate, conditional)	6–20 weeks each	Fixed-fee builds from the backlog, one at a time

What the Agency Provides

- Platform administrator access and accounts issued at award, as a dated government-furnished dependency.
- A product owner with decision authority for two to four hours a week, more during design sign-off.
- An ISSO point of contact who confirms environment placement and the change process early.
- Time from the privacy and records officers for flagged apps.
- A COR with authority to decide within days. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
Governance and triage of one existing Power Platform tenant	Tenant provisioning or hybrid identity setup
Licensing posture review	License purchase or resale
Priced rebuild backlog	Builds, unless bought as follow-ons
Configuration evidence and inventory	Writing the SSP or the authorization package
Unclassified commercial, GCC and (conditionally) GCC High	Classified enclaves; Appian, ServiceNow or Salesforce as lead

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified systems only. Avalon's founder serves as project manager and security lead. The engagement adds one named Power Platform solution architect at the PL-600 level and one named platform developer, hired or subcontracted for the engagement. Avalon has no past federal engagements under this service. FAR 15.305 says an offeror without a record of past performance may not be evaluated favorably or unfavorably on that factor; what protects the agency is a named team, a fixed price and a bounded scope delivered in its own tenant.

Requirement	How it is handled
Solution architect and developer	Named personnel whose platform certifications and investigation level match the agency's requirements, listed in the proposal
GCC High or CUI work	Only with named personnel who have worked in that environment, confirmed before award
Civilian access	Public Trust investigation at the tier the agency requires
Platform	Work happens in the agency's tenant with access the agency provisions; Avalon hosts nothing
Insurance and contract vehicles	Any coverage the solicitation requires is a condition of award; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Market-norm range	Avalon
Legacy form and workflow triage, about 4 weeks	\$15K–\$35K	Firm fixed price; illustrative \$17.1K–\$25.7K
Platform governance and app triage, 8–12 weeks	\$50K–\$150K	Firm fixed price; illustrative \$87K
Simple app build, 6–8 weeks	\$25K–\$60K	Conditional follow-on, firm fixed price
Standard workflow app build, 8–14 weeks	\$60K–\$150K	Conditional follow-on, firm fixed price
Case management build, 14–20 weeks	\$150K–\$350K	Conditional follow-on, priced by release
Sustainment retainer	\$5K–\$25K a month	Optional monthly hour bank

Each engagement sits under the \$350,000 simplified acquisition threshold and can be bought as an open-market purchase, usually with operations and maintenance funds. Purchases between the \$15,000 micro-purchase threshold and the SAT are generally set aside for small business when two or more capable small businesses are expected to compete. Larger work can be subcontracted to Avalon by a prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell hardware, software or licenses.

Prices are fixed against one named tenant with caps on environment count and inventory size, and a dated dependency schedule. One labor-rate table applies across Avalon's Application Development & Modernization services, so a low-code line and an automation line in the same proposal never contradict each other.

Illustration: One Tenant, Ten Weeks

The figures below are planning assumptions for one representative civilian GCC tenant with 9 environments, 310 makers, 230 apps, 540 flows and 55 legacy InfoPath forms and SharePoint 2013 workflows. They are not a quote and not a result from any engagement.

The Governance Gap

Measure	Assumed count	Share
Apps in the default environment	219	95% of apps
Apps whose owner has left	59	26% of apps
Apps using a non-business connector	36	
Apps touching PII	26	
Flows in the default environment	410	76% of flows
Flows mixing business data with non-business connectors	46	

Dispositions and the Rebuild Backlog

Segment	Apps	Disposition
Inactive for 90 days or more	92	Retire, after the records officer confirms retention
Single-user personal tools	58	Leave personal, under default-environment DLP
Active team apps, low sensitivity	44	Promote to a managed environment
Shared apps that touch PII	18	Rebuild as a governed build
Orphaned but still in daily use	14	Rebuild as a governed build
Beyond platform-native scope	4	Route to Process Automation or custom development

Of the 55 legacy forms and workflows, 23 show no use in the past year and retire. The other 32 consolidate with the rebuild candidates above into 11 builds, because several forms usually serve one process.

Build tier	Builds	Band each	Backlog range	Each under the SAT
Simple	6	\$25K–\$60K	\$150K–\$360K	Yes
Standard	4	\$60K–\$150K	\$240K–\$600K	Yes
Case management	1	\$150K–\$350K	\$150K–\$350K	At the ceiling: split by release
Total	11		\$540K–\$1.31M	

The backlog is not one purchase. It is a list the agency funds one build at a time, in the order its own priorities set, each a separate fixed-fee task.

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Inside \$50K–\$150K
Lean (8 weeks)	392	\$52.8K–\$78.2K	\$65K	Yes
Base (10 weeks)	520	\$70.0K–\$103.6K	\$87K	Yes
High sprawl (12 weeks)	780	\$102.0K–\$151.8K	\$127K	Top exceeds: cap inventory

The base case loads the architect and developer at half time, the project manager at one-fifth and 40 hours of security engineering, at \$160 to \$230 an hour for architecture and security, \$110 to \$170 for development and \$120 to \$180 for project management. That is 520 hours, or \$70.0K to \$103.6K. A lean single-environment case runs \$52.8K to \$78.2K. A high-sprawl case runs \$102.0K to \$151.8K; its top touches the band ceiling, so the statement of work caps the inventory and environment count instead of growing the fee. The legacy triage alone, four weeks with a quarter-time architect, a half-time developer and a tenth-time project manager, runs \$17.1K to \$25.7K.

Common Pitfalls

Pitfall	How to avoid it
"One more" app, screen or integration	Freeze the release-1 backlog at design sign-off; everything else goes to the enhancement backlog
Building in the default environment or the wrong cloud	Placement by data type is decision zero, confirmed with the ISSO
Premium licensing found after go-live	Licensing posture is a design deliverable, before any build
Overstating compliance	Platforms are certified; apps are configured and evidenced; the AO decides
Agency dependencies absorbed by the vendor	Every dependency dated in the SOW, with schedule relief
Personal-grade apps shipped as enterprise systems	Promotion criteria: owner, ALM, test evidence and a support model

Conclusion and Next Step

An agency with Microsoft 365 already owns a low-code platform and, in most cases, an unplanned app portfolio inside it. The question is not whether to use low code. It is whether the apps already built are counted, owned, placed in the right environment and governed by rules the ISSO can stand behind.

The natural first step is the fixed-fee governance and app triage: one tenant, about ten weeks, under the simplified acquisition threshold, ending in an environment strategy, applied DLP policy, a full inventory with a disposition for every app, and a priced rebuild backlog. To discuss a tenant, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Default environment

The Power Platform environment every licensed user can build in, created with the tenant.

DLP policy

A data loss prevention rule that groups connectors as business, non-business or blocked, so they cannot be mixed in one app or flow.

Managed environment

A Power Platform environment with added governance controls such as sharing limits and usage insights.

CoE Starter Kit

Microsoft's free governance toolkit that inventories environments, apps, flows, connectors and makers.

ALM

Application lifecycle management: solution packaging, pipelines and release gates from development to production.

Disposition

The decision for each app: retire, leave personal, promote, rebuild or route to another service.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative civilian tenant. None is drawn from a specific agency, a real tenant or a completed engagement.

Assumption	Value	Basis
Tenant	9 environments, 310 makers, 230 apps, 540 flows	Planning assumption
Legacy estate	34 InfoPath forms, 21 SharePoint 2013 workflows	Planning assumption
Loading (base)	Architect 0.5, developer 0.5, PM 0.2 FTE, 40 security hours	KB delivery model
Rates	Architect \$160–\$230, developer \$110–\$170, PM \$120–\$180 an hour	KB market reference
Build bands	\$25K–\$60K, \$60K–\$150K, \$150K–\$350K	KB market norms
Price check	Base fee \$87K	Inside \$50K–\$150K; under the SAT

Appendix C: References

1. **Microsoft**, *Center of Excellence (CoE) Starter Kit*
<https://learn.microsoft.com/en-us/power-platform/guidance/coe/starter-kit>
2. **Microsoft**, *Data loss prevention policies for Power Platform*
<https://learn.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention>
3. **Microsoft**, *Managed Environments overview*
<https://learn.microsoft.com/en-us/power-platform/admin/managed-environment-overview>
4. **Microsoft**, *Power Apps US Government (GCC, GCC High and DoD)*
<https://learn.microsoft.com/en-us/power-platform/admin/powerapps-us-government>
5. **Microsoft**, *Product lifecycle (InfoPath 2013 and SharePoint 2013 workflows)*
<https://learn.microsoft.com/en-us/lifecycle/products/>
6. **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>

7. **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>
8. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
9. **U.S. Access Board**, *Section 508 Standards (ICT Final Rule)*
<https://www.access-board.gov/ict/>
10. **W3C**, *Web Content Accessibility Guidelines (WCAG) 2.2*
<https://www.w3.org/TR/WCAG22/>
11. **Office of Management and Budget**, *M-25-21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, April 2025*
<https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf>
12. **Office of Management and Budget**, *M-26-05, Adopting a Risk-based Approach to Software and Hardware Security, January 23, 2026*
<https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf>
13. **National Archives and Records Administration**, *Records management guidance for agencies*
<https://www.archives.gov/records-mgmt>
14. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
15. **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/>