



Securing Tomorrow's Missions Today.



Licensed Isn't Configured: A Fixed-Fee SCuBA Baseline Assessment for One Microsoft 365 Tenant

SaaS/IaaS Implementation: learn what your cloud tenant actually enforces, what you can fix with licenses you already own, and what the fix will cost, with evidence your ISSM can use.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Licensed Tenants Stay Unconfigured	3
Why It Concentrates in Government	3
The Mandates and the Calendar	4
What the Engagement Does	5
Deliverables	7
Where the Engagement Stops	7
Evidence the ISSM Can Use	8
How an Engagement Runs	9
What the Agency Provides	9
What Is Not Included	10
How Avalon Staffs It	10
Pricing and How to Buy	12
Illustration: One Tenant, One Scan	12
Sorting the Failures	13
What the Engagement Costs	14
Common Pitfalls	15
Conclusion and Next Step	15
Appendices	16
Appendix A: Glossary	16
Appendix B: Illustration Assumptions	16
Appendix C: References	17

Executive Summary

Agencies buy cloud services faster than they configure them. Licenses arrive through a reseller or a product buy at the end of the fiscal year, the tenant gets activated with vendor defaults, and the services that would have hardened it were never funded. Months later the CISO runs CISA's ScubaGear tool for the first time and gets a report full of red.

That gap now has a directive attached. CISA Binding Operational Directive 25-01 (December 2024) requires federal civilian agencies to apply the Secure Cloud Business Applications (SCuBA) secure configuration baselines to in-scope cloud tenants, starting with Microsoft 365, and to report against them. A FedRAMP Certified offering does not close the gap on its own: certification covers the provider's side of the boundary, and the agency still owns every control listed as customer-responsible.

This paper is for the people who carry that problem: CISOs who answer for BOD 25-01 reporting, ISSMs and ISSOs who need configuration evidence they can map to the system security plan, CIOs and cloud program offices who hold the budget, and the CORs who buy the work. It describes Avalon Technology Services' SaaS/IaaS Implementation service, which starts with one engagement:

- **A fixed-fee SCuBA baseline assessment for one Microsoft 365 tenant.** One unclassified civilian tenant, about four billable weeks after access is issued. A ScubaGear run, a walkthrough of the Customer Responsibility Matrix, and a findings register that sorts every failed policy into configuration-only, license-gated or exception. The market band for this work is \$25K to \$75K firm fixed price.
- **A separately priced remediation follow-on.** Configuration-only fixes applied in capped change windows, a post-remediation scan, and an updated configuration workbook keyed to control IDs.

Section 9 works through an illustrative tenant. One scan checks 145 policies across seven products; 52 fail, 34 of them at the SHALL level. 38 of the 52 failures (73%) can be fixed with licenses the agency already owns. The illustrative assessment fee is \$47K, and remediation of the configuration-only items adds about \$41K to \$58K.

The service configures and documents. It produces assessor-ready evidence for customer-responsible controls; CISA's tool scores the tenant, the agency's assessor assesses controls, and the Authorizing Official (AO) decides.

Why Licensed Tenants Stay Unconfigured

The same phrases come up in almost every conversation about a federal tenant, and each one points to the same gap: a product was bought, but the configuration work was not.

What the agency says	What it usually means
"We bought it but it's not stood up."	Licenses arrived through a product buy with no implementation services attached
"The reseller set up the tenant and nobody's touched it since."	Entitlements were activated; secure configuration was never applied
"We can't pass the ScubaGear scan."	Failures have not been sorted into what can be fixed now, what needs a license and what needs a documented exception
"Security won't let us connect it until..."	The ISSM has no configuration evidence mapped to the customer-responsible controls
"Our cloud person left in the RIF."	Nobody on staff holds the tenant's admin history or knows why settings are what they are

Why It Concentrates in Government

- **Purchase and deployment are split.** Fourth-quarter money buys licenses by September 30; the deployment need lands in the next fiscal year with no services funded.
- **Engineering benches are thin.** Workforce reductions left many infrastructure and security teams without staff who hold current Microsoft 365 security skills.
- **Certification is misread.** "It's FedRAMP Certified, so it's secure when we turn it on" confuses the provider's controls with the agency's.
- **Connectivity is engineered.** TIC 3.0 means cloud access follows an approved path, not a default internet connection.

The Mandates and the Calendar

Driver	What it requires	What it means for this engagement
CISA BOD 25-01 (Dec 2024) and the SCuBA baselines	Secure configuration baselines for in-scope cloud tenants, Microsoft 365 first, with reporting to CISA; not replaced by BOD 26-04	The core driver; ScubaGear output is the measuring stick
FedRAMP Consolidated Rules (Jun 25, 2026)	Offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	The agency configures and authorizes its own use through the Customer Responsibility Matrix
NIST SP 800-53 Rev. 5	Controls in AC, IA, AU, CM and SC, plus configuration portions of CP and IR	The control IDs every finding and fix is keyed to
NIST SP 800-37 Rev. 2	RMF Prepare and Implement steps	Where configuration work sits in the authorization lifecycle
TIC 3.0	Security capabilities for cloud use cases	Conditional access and tenant restrictions are part of the review
OMB M-22-09 (Jan 26, 2022)	Zero trust strategy: phishing-resistant MFA and identity-centric access	Identity findings carry the most weight
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Audit log settings and export are checked against the agency's logging decisions
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for known exploited vulnerabilities; replaced BOD 22-01	Applies to connected components the agency runs, not to tenant settings

Driver	What it requires	What it means for this engagement
DoD Cloud Computing SRG and CSRMC (Sep 24, 2025)	Impact-level requirements; RMF, DoDI 8510.01 and eMASS remain in use	Unclassified DoD tenants follow the same evidence pattern; civilian work comes first

The engagement gets bought at predictable moments: a new license buy that landed without services; a ScubaGear finding or a BOD 25-01 reporting gap; late moves off Exchange Server 2016 and 2019, which reached end of support on October 14, 2025; an inspector general or GAO finding on cloud configuration; a mission system blocked at authorization because its environment cannot produce evidence; DoD components working toward target-level zero trust capabilities by the end of FY2027; and fourth-quarter operations and maintenance funds looking for a fixed-price, fast-start use.

What the Engagement Does

A reseller's onboarding activates entitlements. A provider's quick-start turns features on. Neither produces evidence keyed to the agency's Customer Responsibility Matrix. This engagement measures the tenant against the mandatory baselines, explains every failure, and hands the agency a sequenced plan to fix it.

Step	Activities
Kickoff and access	Read-only or paired-hands access agreed, government dependencies dated in writing, success criteria and the in-scope product list confirmed
Discovery	Customer Responsibility Matrix walkthrough, license entitlement review, identity and privileged-role inventory, integration list (identity provider, SIEM export, ticketing, records)
Baseline scan	ScubaGear run against the in-scope products, with agency administrators present; HTML and JSON output retained as the pre-remediation record
Classification	Every failed policy tagged SHALL or SHOULD and sorted into configuration-only, license-gated or exception (a POA&M candidate), with the control IDs it touches
Remediation plan	Fixes sequenced by risk and change-board cadence, with hours and a fixed price for the follow-on
Readout	Briefing to the CISO, ISSM and program office

Identity gets the closest look: federation to the agency identity provider, PIV or CAC and phishing-resistant MFA, who holds global administrator and who should, and break-glass accounts. Where customer-managed keys are in use, the review confirms they rely on FIPS 140-3 validated modules. Tools are no-cost: ScubaGear and Microsoft's own admin centers. Nothing is installed in the tenant.

Deliverables

Deliverable	Format
Pre-remediation ScubaGear report	HTML and JSON as produced by the tool
Configuration workbook mapped to Customer Responsibility Matrix control IDs	Excel, with a Markdown copy
Findings register: policy, product, SHALL or SHOULD, class, control IDs, recommended action	Excel or CSV
Identity and privileged-role record	PDF
Sequenced remediation plan with hours and follow-on price	Word or PDF
Readout	Slide deck and live briefing

Where the Engagement Stops

The assessment does not design a landing zone (Avalon's separate Cloud Architecture & Engineering service), move workloads (Cloud Migration & Development), claim license or consumption savings (FinOps), or onboard the agency to a shared service (Gov-Shared Cloud Services). It does not resell licenses, write the SSP, manage the POA&M or run a security operations center. Avalon's privileged access, if any is granted, ends at closeout by design.

Evidence the ISSM Can Use

Control family	What the engagement documents
AC (access control)	Conditional access policies, tenant restrictions, external sharing and guest access settings
IA (identification and authentication)	Federation, PIV or CAC, phishing-resistant MFA and legacy authentication status (IA-2)
AU (audit and accountability)	Audit log settings, retention and export paths to the agency SIEM
CM (configuration management)	The baseline itself, scan results and deviations (CM-2, CM-6)
SC (system and communications protection)	Encryption in transit (SC-8), key management (SC-12) and data at rest (SC-28) settings the agency controls
CP and IR (configuration portions)	Retention, recovery and alerting settings the tenant exposes

The accurate way to state the value is narrow: the engagement measures the tenant against the mandatory SCuBA baselines as of the scan date and documents the customer-responsible controls in a form an assessor can test. The remediation follow-on implements those controls and delivers an assessor-ready evidence pack keyed to the SSP.

Accurate	Not accurate
Conformance with mandatory SCuBA baselines as of the scan date	Certifies BOD 25-01 or SCuBA compliance
Evidence for customer-responsible controls	A FedRAMP-compliant implementation
An input to the ISSM and the assessor	Achieves or speeds an ATO
A sequenced remediation plan	Guarantees passing an assessment

How an Engagement Runs

Phase	Timing	What happens
Kickoff and access	1–2 weeks	Accounts and access issued, dependency schedule signed, communication cadence set
Discovery	Weeks 1–2 of work	Responsibility matrix walkthrough, entitlements, identity and integration inventory
Scan and classification	Weeks 2–3	ScubaGear run, failure classification, control mapping
Plan and readout	Week 4	Remediation plan, draft register, five-business-day agency review, final briefing
Remediation follow-on (separate)	4–6 weeks	Configuration-only fixes in capped change windows, pilot group first, post-remediation scan

What the Agency Provides

- One point of contact with authority, usually the ISSM or the COR, who can unblock access and scheduling.

- Access for Avalon personnel, or a paired-hands model where agency administrators run the tool. Account and PIV issuance routinely takes two to six weeks, so it is written into the statement of work as a dated government-furnished dependency.
- ISSO or ISSM time of two to four hours a week for control-mapping decisions.
- The current SSP if one exists, license entitlements, network diagrams and the list of integrations.
- Change-board slots reserved in advance for the remediation follow-on. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
Entitlement mapping	License or subscription resale
A remediation plan and price	Remediation, unless bought as the follow-on
Evidence the SSP author can use	Writing the SSP or the authorization package
Exceptions flagged as POA&M candidates	Managing the POA&M
Audit log export settings	Security operations or monitoring
Reviewing an existing landing zone's guardrails, on request	Designing a landing zone or migrating workloads
Unclassified tenants	Classified environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified tenants only. Avalon's founder serves as engagement lead and project manager, with one named, certified Microsoft 365 security engineer. 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. Avalon never serves as the independent assessor of a tenant it configured, and it will sign an organizational conflict of interest representation.

Requirement	How it is handled
Microsoft 365 security engineer	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal, hired or subcontracted
Security lead credential	A CISSP or CCSP holder named in the proposal where the agency requires one
Civilian access	Public Trust investigation at the tier the agency requires, as a condition of the engagement
Scan output handling	Agency-approved handling for scan reports and configuration data before award; nothing over unmanaged email
IaaS guardrail reviews	Offered only with a named engineer certified on the agency's cloud platform
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
SCuBA baseline gap assessment, one tenant, about 4 billable weeks	\$25K–\$75K	Firm fixed price; illustrative \$47K
Configuration-only remediation follow-on, 4–6 weeks	With the assessment: \$60K–\$150K	Firm fixed price from the plan
Small tenant implementation (up to 1,000 seats, light migration)	\$60K–\$150K	Firm fixed price, with a named engineer
Mid tenant implementation (1,000–10,000 seats)	\$150K–\$500K	Up to about 5,000 seats, one engagement at a time
Enterprise or multi-enclave implementation	\$500K–\$2M+	Not offered today

The assessment and its follow-on sit under the \$350,000 simplified acquisition threshold, so both can be bought as open-market purchases. 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. Configuration work inside a larger cloud or zero trust task order can be subcontracted to Avalon by the prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell licenses.

Prices are fixed against named products, a named integration count and capped change windows, with a unit-price menu for additions published at kickoff. The assessment is priced to be an easy first purchase, but not so low that it misstates what the implementation that follows will cost.

Illustration: One Tenant, One Scan

The figures below are a planning illustration for one representative civilian Microsoft 365 tenant, not a quote and not a result from any engagement. Policy counts and scan results are assumptions, not CISA's current catalog; the live baselines and the BOD 25-01 required-configurations list govern any real scan.

Product	Policies	Pass	Fail	Manual	Fail rate	SHALL fails
Entra ID	30	14	12	4	46%	9
Defender	25	12	10	3	46%	6
Exchange Online	35	20	11	4	36%	7
SharePoint and OneDrive	10	6	3	1	33%	2
Teams	25	15	8	2	35%	5
Power Platform	10	4	5	1	56%	4
Power BI	10	5	3	2	38%	1
Total	145	76	52	17	41%	34

Fail rate counts only automated checks, so the 17 policies that need manual review are set aside and confirmed by hand. Power Platform has the highest fail rate at 56%, but Entra ID carries the most SHALL failures, and identity findings lead the plan because M-22-09 makes phishing-resistant MFA the first identity priority.

Sorting the Failures

Class	Failures	What happens next
Configuration-only	38	Fixed with licenses the agency already owns, in the remediation follow-on
License-gated	8	A decision memo for the program office: buy the feature, or document an alternative
Exception	6	A written rationale and compensating control, handed to the ISSM as a POA&M candidate
Total	52	34 SHALL and 18 SHOULD

73% of the failures need no new spending. That is usually the most useful number in the readout, because it separates the configuration problem from the budget problem. The license-gated items typically involve privileged identity management and risk-based conditional access, which need a higher license tier; the exceptions are settings a mission partner relationship depends on, such as external Teams access.

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Fits \$25K–\$75K
Lean (3 weeks)	210	\$29.2K–\$41.0K	\$35K	Yes
Base (4 weeks)	280	\$39.0K–\$54.6K	\$47K	Yes
Heavy (6 weeks)	420	\$58.5K–\$81.9K	\$70K	No: cap scope

The base case is four billable weeks: 40 hours of engagement lead at \$170 to \$240, 160 hours of senior cloud engineering at \$140 to \$195, 40 hours of compliance support at \$120 to \$170, and 40 hours of project management at \$125 to \$175. That is 280 hours, or \$39.0K to \$54.6K, with a \$47K planning fee at the midpoint. A six-week scope breaks the \$75K top of the band, so the statement of work caps products and integrations instead. A second tenant or enclave adds 30% to 60%, or \$50.7K to \$87.4K. Every case sits far below the simplified acquisition threshold.

The remediation follow-on prices from the register: 38 configuration-only fixes at 3 hours each, 8 license decisions at 2, 6 exception write-ups at 4, fixed blocks for change-board packages, pilot-group validation, the post-remediation scan and the workbook update, and 15% project management: 297 hours, or \$41.4K to \$57.9K at the same blended rates. Assessment and remediation together run 577 hours and \$80.4K to \$112.5K, inside the \$60K to \$150K band for a small tenant implementation.

Common Pitfalls

Pitfall	How to avoid it
Access issuance slips	Date it as a government-furnished dependency; schedule moves day for day
Integration drift ("just one more system")	Name every integration in the statement of work
"While you have global admin" side tasks	Change-order menu with unit prices published at kickoff
Environment multiplication	One named tenant; a second tenant or enclave is priced separately
Governance by request	A RACI that ends Avalon's role at handoff, and access that expires at closeout
"Just take a quick look at our tenant"	No access or data before award; the paid assessment is the quick look
Assessing your own work	Bid the implementation or the independent assessment on a tenant, not both
Overselling the result	Use the accurate phrasing; CISA's tool scores, the assessor assesses, the AO decides

Conclusion and Next Step

A licensed tenant is not a configured one, and a configured tenant without evidence is not one the ISSM can defend. Most agencies already own the features the SCuBA baselines ask for. What they lack is a clear list of what is failing, which failures cost nothing to fix, and a fixed price for fixing them.

The natural first step is the fixed-fee SCuBA baseline assessment: one Microsoft 365 tenant, about four billable weeks, under the simplified acquisition threshold, ending in a ScubaGear record, a classified findings register, a configuration workbook keyed to control IDs and a priced remediation plan. To discuss a tenant, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

BOD 25-01

CISA Binding Operational Directive 25-01, Implementing Secure Practices for Cloud Services (December 2024).

Customer Responsibility Matrix (CRM)

The provider's list of controls the customer agency must implement or share when using a FedRAMP Certified offering.

SCuBA

CISA's Secure Cloud Business Applications project, which publishes secure configuration baselines for cloud business applications.

ScubaGear

CISA's open-source tool that checks a Microsoft 365 tenant against the SCuBA baselines and reports in HTML and JSON.

SHALL and SHOULD

Baseline policy levels: SHALL policies are mandatory; SHOULD policies are recommended.

TIC 3.0

CISA's Trusted Internet Connections program guidance, including security capabilities for cloud use cases.

Paired hands

An access model where agency administrators make changes while the contractor directs and documents.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative civilian Microsoft 365 tenant. None is drawn from a specific agency, a real scan or a completed engagement.

Assumption	Value	Basis
Products and policies	7 products, 145 policies	Assumed for the illustration, not CISA's current count
Scan result	76 pass, 52 fail, 17 manual	Planning assumption
Failure classes	38 configuration-only, 8 license-gated, 6 exception	Planning assumption
Assessment hours	40 lead, 160 engineer, 40 compliance, 40 PM	Four billable weeks
Rates	\$120–\$240 an hour by role	Category rate card, unclassified
Remediation hours	3, 2 and 4 per failure by class; 104 fixed; 15% PM	Planning assumption
Second tenant	+30% to +60%	KB scaling rule for a second enclave
Price check	Base fee \$47K	Inside the \$25K–\$75K band

Appendix C: References

4. **Cybersecurity and Infrastructure Security Agency**, *BOD 25-01, Implementing Secure Practices for Cloud Services*
<https://www.cisa.gov/news-events/directives/bod-25-01-implementing-secure-practices-cloud-services>
5. **Cybersecurity and Infrastructure Security Agency**, *Secure Cloud Business Applications (SCuBA) Project*
<https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project>
6. **Cybersecurity and Infrastructure Security Agency**, *ScubaGear*
<https://github.com/cisagov/ScubaGear>

7. **Cybersecurity and Infrastructure Security Agency**, *Trusted Internet Connections (TIC) 3.0*
<https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic>
8. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
9. **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>
10. **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>
11. **Office of Management and Budget**, *M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>
12. **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>
13. **Tenable**, *CISA BOD 26-04 FAQ: Vulnerability Remediation Impact, June 11, 2026*
<https://www.tenable.com/blog/cisa-bod-26-04-FAQ-vulnerability-remediation-impact>
14. **Defense Information Systems Agency**, *DoD Cloud Computing Security Requirements Guide*
<https://public.cyber.mil/dccs/>
15. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
16. **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/>