



Securing Tomorrow's Missions Today.



Everything Is Rated High: A Fixed-Fee Threat Model and Risk Evaluation for One System Before Reauthorization

Risk Evaluation & Threat Modeling: know which threats matter most to your system, why, and what to fix first, with RA-3 evidence your Authorizing Official can trace.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Every Register Drifts to High	3
Why It Concentrates in Government	3
The Mandates and the Calendar	5
What the Engagement Does	6
Deliverables	8
Where the Engagement Stops	8
Evidence the AO Can Trace	9
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	14
Illustration: From 84 Highs to a Ranked List	14
The Top of the Remediation Roadmap	16
What the Engagement Costs	17
Common Pitfalls	18
Conclusion and Next Step	18
Appendices	19
Appendix A: Glossary	19
Appendix B: Illustration Assumptions	19
Appendix C: References	20

Executive Summary

Every federal system needs a current risk assessment to keep its authorization. In practice, many of those assessments are the same document from three years ago with new dates, and the risk register behind them rates nearly every item High. When everything is High, nothing is. The Authorizing Official (AO) cannot see which exposures matter, the ISSM cannot defend the residual risk statement, and remediation money follows scanner severity scores instead of the threats that could actually stop the mission.

NIST SP 800-30 Rev. 1 already describes the fix: identify credible threat sources and events, judge how likely each is to cause harm and how bad the harm would be, and rank the results on the agency's own scale. Control RA-3 in NIST SP 800-53 Rev. 5 requires that assessment and its refresh after significant change. What is usually missing is the engineering underneath: a threat model of how the system is actually built, so that each rating traces to a named attack path instead of an assessor's judgment.

This paper is for the people who carry that problem: ISSMs and ISSOs who own the authorization package, CISOs who fund the work, system owners and program managers whose system is changing, and the CORs who buy it. The AO rarely signs the purchase but drives it, because the ISSM buys what the AO will accept. It describes Avalon Technology Services' Risk Evaluation & Threat Modeling service, which starts with one engagement:

- **A fixed-fee combined threat model and SP 800-30 risk evaluation for one system.** One moderate-impact FISMA system, unclassified or Public Trust, over six to nine weeks. Threat modeling with STRIDE, PASTA or LINDDUN, mapped to MITRE ATT&CK, feeds an 800-30 risk register formatted for eMASS, CSAM or Xacta. Avalon prices it at \$60K to \$85K firm fixed price, inside a \$60K to \$120K market band.
- **Conditional follow-ons.** An annual refresh at 40% to 60% of the initial price, and a FAIR quantification annex only once an OpenFAIR-credentialed analyst is named.

Section 9 works through an illustrative system. The agency's existing register holds 120 items, 84 of them rated High. The engagement groups that evidence under 40 threat scenarios and scores each one. 6 scenarios (15%) come out High or Very High, and those lead the remediation roadmap. The illustrative fixed fee is \$78K.

The service analyzes evidence the agency already has. It runs no scans and no exploitation, and it does not generate new technical findings; its threat model tells a later test, such as Avalon's separate Vulnerability Assessment & Exploitation or network testing services, where to aim. It produces RA-3 evidence. The agency's assessor assesses controls, and the AO decides.

Why Every Register Drifts to High

Stale and inflated risk assessments show up in the same phrases across agencies. Each one points to the same gap: findings without analysis.

What the ISSM says	What it usually means
"Our risk assessment is basically the same document from three years ago."	The RA-3 artifact was re-dated at reauthorization, not re-analyzed, even though the architecture changed
"Everything in our register is rated high, so nothing is."	Ratings were copied from scanner severity, with no likelihood judgment for this system and its threats
"The AO keeps asking questions our POA&M can't answer."	Open items list weaknesses but not the threat events that would exploit them or the mission harm that would follow
"We have terabytes of scan data and no way to prioritize it."	Scan data is evidence, not analysis; nobody has tied it to attack paths
"We're going through reauthorization next spring."	The risk picture the AO will sign on needs to be current before the package is assembled

Why It Concentrates in Government

- **Legacy systems with undocumented connections.** Few people on staff hold a complete picture of how data moves through the system or where it crosses a trust boundary.
- **ISSO time goes to paperwork.** Continuous monitoring and data calls absorb the hours that analytical work needs.

- **The process rewards an artifact.** Reauthorization cycles create a predictable temptation to update dates rather than analysis.
- **Free capacity is limited.** CISA's no-cost assessment capacity is constrained and its queues are long, so many systems wait or go without.

The Mandates and the Calendar

Driver	What it requires	What it means for this engagement
FISMA (44 U.S.C. § 3554) and OMB Circular A-130	Periodic assessments of risk and risk-based protection decisions	The statutory basis for the work
NIST SP 800-53 Rev. 5, RA-3	Risk assessment, documented and updated on a defined frequency and on significant change	The core control; the engagement produces its evidence
NIST SP 800-30 Rev. 1 and SP 800-37 Rev. 2	The risk assessment method; RMF tasks P-14 (system-level risk assessment), R-2 and R-3	The method followed end to end; outputs feed the AO's risk determination and response
NIST CSF 2.0 (Feb 2024)	Govern function and ID.RA risk assessment outcomes	The frame for CSF-aligned agency reporting
OMB M-19-03	High Value Asset program expectations	HVA designation raises the bar for the system's risk picture
CISA BOD 26-04 (Jun 10, 2026) and BOD 26-02 (Feb 6, 2026)	Risk-based remediation clocks for exploited vulnerabilities; end-of-support edge devices retired on a schedule	Known exploitation and unsupported edge devices raise likelihood ratings
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Logging and detection coverage are inputs to likelihood
DoD CSRMC (Sep 24, 2025)	Cybersecurity risk management construct announced; RMF, DoDI 8510.01 and eMASS remain in use	For unclassified DoD systems, the register goes into the existing eMASS record

The engagement gets bought at predictable moments: a reauthorization six to twelve months out; an RA-3 artifact past its refresh, or a significant change such as a cloud migration or a major release; an inspector general, GAO or FISMA finding on risk management; an incident or near miss leadership wants explained in risk terms; a new system or AI capability entering the RMF; or a zero trust effort that stalled because nobody could say what the architecture defends against. Fall inspector general audit season drives demand into the first half of FY2027, and DoD components face the end-of-FY2027 deadline for target-level zero trust capabilities.

What the Engagement Does

Most offerings in this market sell half the job: a compliance-style 800-30 document built from interviews, or a developer-style threat model of one application that never reaches the authorization package. This engagement runs both workstreams on the same system and uses the threat model as the evidence base for every risk rating.

Workstream	Activities
A. System decomposition	Data flow diagrams, trust boundaries, entry points, privilege levels, external dependencies and data types (CUI, PII, PHI), built from architecture documents and confirmed with the agency's engineers
A. Threat enumeration	STRIDE-per-element for application and API systems, PASTA where business impact drives staging, LINDDUN where privacy threats to PII or PHI are in scope, and attack trees for the most valuable functions
A. ATT&CK mapping	Threats mapped to MITRE ATT&CK techniques so detection and hunt teams can act on the model; abuse cases tied to existing or recommended 800-53 controls
B. Characterization	FIPS 199 categorization validated or challenged, not simply accepted; information types framed by mission impact
B. Threat sources and events	All four 800-30 classes: adversarial, accidental, structural and environmental
B. Vulnerability analysis	The agency's existing evidence (scan exports, prior assessment reports, open POA&M items, configuration baselines) correlated against the threat model
B. Likelihood, impact and risk	Scored per 800-30 Appendices G through I, calibrated to the agency's own risk scale; a prioritized register with accept, avoid, mitigate or transfer responses mapped to controls

Delivery uses no-cost tools: ATT&CK Navigator, OWASP Threat Dragon, the Microsoft Threat Modeling Tool and draw.io. Avalon holds no commercial threat modeling license such as IriusRisk. Nothing is installed in the agency environment; the work needs read-only document access and workshop time.

Deliverables

Deliverable	Format
Risk Assessment Report: method, threat sources and events, likelihood and impact analysis, risk determinations, recommended responses	Word and PDF, with an executive summary
Risk Register	Excel or CSV structured for import into eMASS, CSAM or Xacta
Threat Model Package: DFDs, trust boundaries, per-element threats, abuse cases	draw.io or Visio source plus PDF; Threat Dragon project files where used
ATT&CK coverage layer	ATT&CK Navigator JSON plus PDF
Prioritized Remediation Roadmap: 30, 60 and 90-day and out-year actions with controls and owners	Word or PDF plus an Excel tracker
Executive Briefing	Slide deck and live outbrief to the CISO and AO level
FAIR quantification annex (optional, conditional on a named OpenFAIR analyst)	PDF annex and model workbook

Where the Engagement Stops

This service analyzes and prioritizes evidence that already exists. The moment new technical evidence is needed (a scan, a penetration test, an exploit), that work is scoped separately, under the agency's written authorization and signed rules of engagement, through Avalon's Vulnerability Assessment & Exploitation or network testing services or another provider. The threat model makes that later test sharper, because it names the entry points and attack paths worth targeting. The routing question at the start of every conversation is simple: does the agency need analysis of evidence it already has, or new evidence generated?

Evidence the AO Can Trace

Control or task	Evidence the engagement produces
RA-3	The 800-30 risk assessment report and register, dated, with the method stated
RA-3(1)	Supply chain threat sources and dependencies identified in the decomposition
RA-2	FIPS 199 categorization reviewed as an input, with any challenge documented
RA-7	Recommended risk responses for each register entry
RA-9	Critical functions and components identified in the threat model
PM-9, PM-28	Risk framing aligned to the agency's risk management strategy and scale
SA-8, SA-11(2)	Threat model and abuse cases for systems in design or development
RMF P-14, R-2, R-3	System-level risk assessment that informs the AO's risk determination and response

The accurate way to state the value is narrow: the engagement produces the NIST SP 800-30-conformant risk assessment and system threat models that satisfy the evidentiary requirements of control RA-3 and inform the AO's risk determination under RMF tasks R-2 and R-3.

Accurate	Not accurate
RA-3 evidence for the authorization package	Grants, guarantees or speeds an ATO
A prioritized, traceable risk register	A security control assessment
A threat model that targets later testing	Penetration test evidence
An input to the AO's risk-acceptance decision	The risk-acceptance decision itself

How an Engagement Runs

Phase	Timing	What happens
Kickoff and scoping	Week 1	Confirm the boundary by FISMA system ID, finalize the data call, agree the risk scale and report template with the ISSM, schedule interviews and workshops
Discovery and characterization	Weeks 2–3	Document review (SSP, diagrams, prior assessments, scan exports, POA&M, interconnection agreements); 6 to 12 interviews of 60 to 90 minutes
Threat modeling workshops	Weeks 3–5	Two to four working sessions with engineers: decomposition, threat enumeration, ATT&CK mapping
Risk analysis	Weeks 5–7	Likelihood and impact scoring, correlation with existing evidence, risk determination, control and remediation mapping, internal QA
Reporting and briefing	Weeks 7–9	Draft report, five-business-day agency review, final report, executive outbrief
Optional re-check	60 or 90 days later, 1 week	Check remediation of top risks and refresh the register

What the Agency Provides

- One point of contact with authority, usually the ISSM or the COR, who can unblock access and scheduling.
- The current SSP, architecture and network diagrams, asset inventory, latest scan exports and open POA&M, within 10 business days of kickoff.
- Six to twelve stakeholders for one interview each, and engineers at two to four workshops.

- Document and meeting access by week 2, and a five-business-day turnaround on the draft report.
- About 40 to 70 agency staff-hours in total. Agency-caused delays move the schedule day for day, and data-call items more than 10 business days late trigger a re-plan.

What Is Not Included

Included	Separate work
Analysis of existing scan exports and reports	Active scanning or new discovery
A threat model that names what to test	Exploitation, red teaming or penetration testing
Inputs the SSP author can use	Writing or rewriting the SSP
Seeding the POA&M with register findings	Managing the POA&M
A prioritized remediation roadmap	Performing the fixes
A point-in-time assessment of one system	Continuous monitoring or threat hunting
Evidence for the assessor and the AO	The control assessor role, certification or any authorization decision
Unclassified or Public Trust systems	Classified systems and intelligence community work

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 engagement lead and project manager, with one named threat modeling and risk analyst. 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 schedule. Avalon never assesses a system it built or operates, and it will sign an organizational conflict of interest representation.

Requirement	How it is handled
Threat modeling and risk analyst	Named personnel whose certifications (CISSP at minimum) and investigation level match the agency's requirements, listed in the proposal, hired or subcontracted
FAIR annex	Offered only when an OpenFAIR-credentialed analyst is named in the proposal
Civilian access	Public Trust investigation at the tier the agency requires, as a condition of the engagement
Workpaper handling	Agency-approved handling for any CUI, PII or PHI in workpapers in place before award; no sensitive material over unmanaged email
DoD CUI-heavy scopes	Not pursued until Avalon has a NIST SP 800-171 self-assessment score in SPRS
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
Combined threat model and 800-30 risk evaluation, one moderate system, 6–9 weeks	\$60K–\$120K	\$60K–\$85K firm fixed price
Focused threat model, one application or system, 3–5 weeks	\$25K–\$60K	Firm fixed price
Single-system 800-30 risk assessment, 6–9 weeks	\$40K–\$90K	Firm fixed price
Annual refresh, 3–5 weeks (conditional)	40%–60% of the initial price	Firm fixed price
FAIR quantification annex, +2 weeks (conditional)	+\$15K–\$35K	Only with a named OpenFAIR analyst
Portfolio of 3–5 systems or HVA-grade work	\$150K–\$400K+	Not offered today

Every Avalon tier sits under the \$350,000 simplified acquisition threshold, so it can be bought as an open-market purchase. 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. Risk work inside a larger authorization 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.

Operations and maintenance funds buy most of this work, which makes the third and fourth quarters a natural window. Threat modeling for a system in development rides the program's RDT&E funding and follows its milestones. Performance-based pricing is declined: assessment quality is hard to contract as an outcome without bad incentives, and a fixed price against a capped scope keeps them clean.

Illustration: From 84 Highs to a Ranked List

The figures below are a planning illustration for one representative moderate-impact system, not a quote and not a result from any engagement. Every scenario, rating and hour is an assumption.

The agency hands over a register and POA&M of 120 open items, 84 of them (70%) rated High, mostly carried over from scanner severity. The engagement does not re-rate those items one by one. It builds 40 threat scenarios from the threat model, attaches each existing item to the scenarios it enables as evidence, and scores the scenarios with the 800-30 likelihood and impact scales and the Appendix I risk matrix.

Risk level	Scenarios	Share
Very High	1	2%
High	5	12%
Moderate	14	35%
Low	14	35%
Very Low	6	15%
Total	40	100%

6 of 40 scenarios (15%) rate High or Very High. The scenarios span all four 800-30 source classes: 27 adversarial, 6 accidental, 4 structural and 3 environmental. A QA rule backs the distribution: if more than 25% of scenarios land at High or above, the team rechecks calibration against the agency's scale before the draft goes out. The point is not a quota; it is that every High has to be argued from a named attack path and a stated mission impact.

The Top of the Remediation Roadmap

#	Scenario	L / I	Risk	Control	Owner	Horizon
1	Exploitation of an end-of-support VPN appliance at the boundary	H / VH	Very High	SA-22	Network operations	30-day
2	Phishing for administrator credentials where MFA is not phishing-resistant	H / H	High	IA-2	Identity team	60-day
3	Exploitation of a known exploited vulnerability on the public web tier	H / H	High	SI-2	System administrators	BOD 26-04 clock
4	Bulk export of PII through an over-privileged API service account	M / VH	High	AC-6	Application team	60-day
5	Ransomware with backups reachable from the production domain	M / VH	High	CP-9	Infrastructure team	60-day
6	Password spraying against the public sign-in portal	H / M	Moderate	AC-7	Identity team	90-day
7	Abuse of a partner interconnection to reach internal services	M / H	Moderate	CA-3	ISSO and partner POC	90-day
8	Harvesting of records from misconfigured cloud object storage	M / H	Moderate	AC-3	Cloud operations	90-day

The end-of-support VPN appliance leads because known exploitation of edge devices makes the likelihood High and the impact reaches the whole boundary; BOD 26-02 also puts a retirement date on it. The public web tier item follows the agency's BOD 26-04 clock rather than the roadmap's horizon. The highlighted adversarial scenarios map to 9

ATT&CK techniques, and that layer goes to the SOC and to any later penetration test as a target list. The Excel tracker carries the rest of the register with owners and dates.

What the Engagement Costs

Scenario	Interviews / workshops / DFD elements / scenarios	Hours	Rate-band range	Planning fee
Lean	6 / 2 / 20 / 30	386	\$58K–\$100K	\$68K
Base	9 / 3 / 30 / 40	448	\$67K–\$116K	\$78K
Heavy	12 / 4 / 45 / 60	534	\$80K–\$139K	\$93K

The base case adds up interviews (36 hours), workshops (42), STRIDE-per-element enumeration of 30 DFD elements (45), scoring 40 scenarios (60), fixed blocks for scoping, document review, ATT&CK mapping, the register and roadmap, and reporting (224), plus 10% project management: 448 hours, or about 56 hours a week across two people over eight weeks. At a \$175 planning rate that is \$78K, inside Avalon's \$60K to \$85K anchor. Across the \$150 to \$260 blended band it runs \$67K to \$116K, inside the \$60K to \$120K market band. A lean scope prices at the \$60K floor. A heavy scope reaches \$93K at the planning rate and breaks the anchor, so the statement of work caps interviews, workshops and scenario count and prices additions by modification. Every case sits well under the simplified acquisition threshold. An annual refresh of the base case would run about \$31K to \$47K.

Common Pitfalls

Pitfall	How to avoid it
Boundary drift	Name the FISMA system ID; interconnected systems appear as threat sources only
Workshop multiplication	Cap the workshop count in the statement of work
"While you're here, can you run a scan?"	New evidence is separate testing work under its own authorization
Remediation drift	The roadmap is the boundary; fixes are separate work
Rating everything High	Calibrate to the agency's scale and apply the QA distribution check
Ignoring the agency's risk scale	Agree the scale and template with the ISSM in week 1
PDF-only artifacts	Deliver the register in import-ready Excel or CSV
Overselling the result	Use the accurate phrasing; the assessor and the AO decide

Conclusion and Next Step

A risk register where everything is High gives the AO nothing to decide with. A register where each rating traces to a named attack path, a likelihood argument and a mission impact gives the AO a real choice, gives the ISSM a residual risk statement they can defend, and gives the CISO a reason to move money to the few things that matter.

The natural first step is the fixed-fee combined engagement: one moderate-impact system, six to nine weeks, under the simplified acquisition threshold, built on the agency's existing evidence, ending in an 800-30 report, an import-ready register, a threat model package, an ATT&CK layer and a ranked roadmap. To discuss a system, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

ATT&CK

MITRE's knowledge base of adversary tactics and techniques, used to map threats so defenders and testers can act on them.

Data flow diagram (DFD)

A diagram of processes, data stores, external entities and the flows between them, with trust boundaries marked.

FAIR

Factor Analysis of Information Risk, a method for expressing risk as ranges of loss frequency and magnitude.

LINDDUN

A privacy threat modeling method for systems that handle personal data.

PASTA

Process for Attack Simulation and Threat Analysis, a staged, business-impact-driven threat modeling method.

STRIDE

Spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege; applied per DFD element.

Threat scenario

A threat source, the event it causes and the weaknesses it uses, scored as one unit for likelihood and impact.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Interviews	9 at 1.25 hours, two staff, plus 1.5 hours of notes each	Planning assumption within the KB's 6–12
Workshops	3 at 3 hours, two staff, plus 8 hours of prep and synthesis each	Planning assumption within the KB's 2–4

Assumption	Value	Basis
Decomposition and scoring	30 DFD elements and 40 scenarios at 1.5 hours each	Planning assumption
Fixed blocks	Scoping 16, document review 40, ATT&CK 24, register and roadmap 40, reporting 104 hours	Planning assumption
Project management	10% of delivery hours	Planning assumption
Existing register	120 items, 70% rated High	Planning assumption
Risk levels	800-30 Rev. 1 Appendix I matrix; QA recheck above 25% High or Very High	Model rule
Rates	\$150–\$260 an hour blended; fee at a \$175 planning rate	KB market-norm band
Price check	Base fee \$78K	Inside the \$60K–\$85K anchor

Appendix C: References

1. **National Institute of Standards and Technology**, *SP 800-30 Rev. 1, Guide for Conducting Risk Assessments*, September 2012
<https://csrc.nist.gov/pubs/sp/800/30/r1/final>
2. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*, December 2018
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
3. **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>
4. **National Institute of Standards and Technology**, *SP 800-39, Managing Information Security Risk*
<https://csrc.nist.gov/pubs/sp/800/39/final>

5. **National Institute of Standards and Technology**, *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*
<https://csrc.nist.gov/pubs/fips/199/final>
6. **National Institute of Standards and Technology**, *Cybersecurity Framework 2.0*
<https://www.nist.gov/cyberframework>
7. **U.S. Code**, 44 U.S.C. § 3554, *Federal agency responsibilities*
<https://www.law.cornell.edu/uscode/text/44/3554>
8. **Office of Management and Budget**, *M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*
<https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf>
9. **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>
10. **Cybersecurity and Infrastructure Security Agency**, *Known Exploited Vulnerabilities Catalog*
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
11. **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>
12. **MITRE**, *ATT&CK*
<https://attack.mitre.org>
13. **OWASP**, *Threat Dragon*
<https://owasp.org/www-project-threat-dragon/>
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/>