



Securing Tomorrow's Missions Today.



Assessor-Ready by Design: Closing Dash-One Findings Without Boilerplate

Security Policy & Procedure Development: interview-driven policies and procedures, mapped control by control and delivered as signature-ready drafts.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Dash-One Findings Stall Authorizations	3
Why It Concentrates in Government	3
How the Need Sounds	4
The 2026 and 2027 Calendar	4
What the Service Does	5
Interviews Are the Method	6
What a -1 Control Asks For	7
Evidence Assessors Can Use	7
How an Engagement Runs	8
What the Agency Provides	9
What Is Not Included	9
How Avalon Staffs It	9
Pricing and How to Buy	10
Illustration: Sizing a Dash-One Sprint	11
Reviewers Set the Critical Path	13
If the Suite Only Needs a Refresh	13
Common Pitfalls	14
Conclusion and Next Step	14
Appendices	15
Appendix A: Glossary	15
Appendix B: Illustration Assumptions	15
Appendix C: References	16

Executive Summary

Federal systems often reach an assessment with protections in place and the paperwork behind them missing, stale or generic. In NIST SP 800-53 Rev. 5, the -1 control in each family requires documented policy and procedures, a designated official to manage them, and review on a defined schedule. A missing or boilerplate -1 is a finding before the assessor reaches a single technical control, and a run of them can stall a reauthorization that is otherwise sound.

The calendar adds pressure. CISA's BOD 26-04 (June 10, 2026) asks civilian agencies to update vulnerability management policy at once, processes within 60 days and full remediation timelines within about 180 days. OMB M-26-14 (May 2026) replaced M-21-31 with a risk-based logging model, so audit and logging policies written to the old tiers are now out of date. BOD 26-02 puts deadlines on end-of-support edge devices. Each of these lands first in a policy or a procedure.

This paper is written for ISSMs and ISSOs, CISOs, system owners, CIO governance offices and the contracting staff who buy the work. It describes Avalon Technology Services' Security Policy & Procedure Development service:

- **Interview-driven drafting.** Avalon interviews the people who do the work, then writes policies and role-assigned procedures that describe real practice, in the agency's directives template, mapped to each control and 800-53A assessment objective.
- **Two shapes.** A bundled workstream of 3 to 6 weeks inside an authorization or RMF effort, or a standalone fixed-price sprint of 4 to 10 weeks. Two adjudication rounds are included; more are priced per round in advance.

Section 9 sizes an illustrative sprint for one system: 18 families in scope, 16 policies to rewrite or refresh and 7 procedures, for about 349 hours over 10 weeks and a fixed price of \$62K. It also shows the variable that moves the schedule most: how fast the agency's reviewers return comments.

The service drafts. The agency adjudicates, signs and issues. Avalon does not assess controls, certify compliance or grant an authorization; those decisions belong to the agency's assessor and Authorizing Official.

Why Dash-One Findings Stall Authorizations

Risk	How it shows up
Compliance	Assessors examine the -1 control in every family in scope. Missing, outdated or untailored policy produces findings across the board, and each becomes a POA&M item for the ISSM to track.
Mission	A system waiting on its authorization cannot deploy or keep operating past expiry. When the package stalls on documentation, the mission capability stalls with it.
Continuity	Practice that lives in one ISSO's head leaves with that ISSO. Written, role-assigned procedures are what a successor inherits.
Scorecard	In the IG FISMA maturity model, Level 2 (Defined) means policies and procedures are formalized and documented. Agencies can sit at Level 1 for documentation reasons alone.

Why It Concentrates in Government

- **A statutory floor.** FISMA (44 U.S.C. § 3554) and OMB Circular A-130 require agencywide security policies and procedures whether or not anyone is staffed to write them.
- **Revision churn.** The move from 800-53 Rev. 4 to Rev. 5, 800-171 Rev. 3 for nonfederal systems, and each new directive put existing documents on a decay schedule the agency does not control.
- **Thin staffing.** Small agencies and components often run on one or two ISSOs. When operations and documentation compete for the same hours, documentation loses.
- **Slow issuance.** Formal policy often routes through legal, records and stakeholder review. Drafts can be out of date by the time they issue.
- **Template packs.** Purchased templates that were never tailored are exactly what assessors and inspectors general call boilerplate.

How the Need Sounds

"We do it; it's just not written down." "The assessor hit us on the dash-ones." "Our ISSO left and took everything with them." "Our policies still say Rev. 4." "Legal has been sitting on our draft for eight months." Each of these is this service.

The 2026 and 2027 Calendar

Date	Event	Policy and procedure impact
September 24, 2025	DoD announces the Cybersecurity Risk Management Construct (CSRMC)	RMF, DoDI 8510.01 and eMASS remain in use; policy suites written to RMF stay valid while components track the transition
February 6, 2026	CISA BOD 26-02: end-of-support edge devices	Inventory in 3 months, decommission in 12, replace in 18; asset lifecycle and acquisition policy (CM-1, SA-1) must say how
May 2026	OMB M-26-14 replaces M-21-31	Risk-based logging model; audit and accountability policy and the log review procedure (AU-1, AU-6) need rewriting
June 10, 2026	CISA BOD 26-04 replaces BOD 22-01 and BOD 19-02	Policy updates immediately, processes within 60 days, full timelines within about 180 days; risk assessment and flaw remediation documents (RA-1, SI-1) change
June 25, 2026	FedRAMP Consolidated Rules published	"FedRAMP Certified" classes A to D cover the provider's offering only; the agency's own policies still govern its systems
July 13, 2026	CMMC Phase 2 suspended	Phase 1 self-assessment and NIST SP 800-171 obligations remain, documentation included
September 30, each year	O&M funds expire	Small, fixed-price documentation buys close in July through September

Date	Event	Policy and procedure impact
June 11, 2027	FedRAMP stops accepting new Rev5 submissions	Agencies sponsoring cloud offerings align documentation to the new rules
End of FY2027	DoD target-level zero trust capabilities due	Identity, access and network policy rewritten on every system zero trust touches

None of these dates is a policy deadline by itself. Each changes what the policy or procedure has to say, and an assessor reading the suite next year will read it against the requirement in force at that time.

What the Service Does

What separates this service from a template pack is that every document is built from interviews and traced to a specific control requirement.

Activity	What happens
Gap assessment	Every existing policy, procedure and standard cataloged and mapped to the target revision; a finding-by-finding gap report that doubles as the drafting plan
Practice-capture interviews	Structured sessions with the ISSO or ISSM, administrators, HR, physical security and acquisition staff, grouped by family cluster, about 2 to 3 hours of agency time per cluster
Policy drafting	One policy per family, or the agency's consolidated structure, in the agency's directives template: purpose, scope, roles, statements traceable to controls, enforcement and review cadence
Procedure drafting	Step-level, role-assigned, tool-specific SOPs for the operational families
Traceability matrix	Every policy statement and procedure step mapped to its control and 800-53A assessment objective
Adjudication management	Comment matrices, a written disposition for every comment, two structured review rounds on a published schedule
Governance wiring	Document owners, version conventions and a review calendar matched to each -1 control's review frequency
Handoff briefing	A 30 to 45 minute session for leadership: what was delivered, what changed and how to keep the suite current

Interviews Are the Method

Assessors interview staff and compare the answers with the documents. A policy that describes what people actually do survives that cross-check; a recycled template fails exactly there. Where interviews show that practice must change to meet the control, the document says so and the gap report records it, rather than describing practice that does not exist. If a budget cannot support interviews, the right response is fewer families in scope, not a weaker method.

What a -1 Control Asks For

Each Rev. 5 -1 control asks for the same three things: policy and procedures that are developed, documented and disseminated; an official designated to manage them; and review and update on a defined frequency and after defined events. The governance charter and review calendar answer the second and third parts, which are the ones most often missing when a suite was written once and left alone. PM-1 is the exception: it covers the information security program plan, which is usually an agency-level document.

Evidence Assessors Can Use

Framework hook	What the deliverables support
NIST SP 800-53 Rev. 5, the -1 control in each family	Policy suite, procedures, designated officials and review calendar
NIST SP 800-53A Rev. 5 examine procedures	Traceability matrix down to the assessment objective, so the examine step moves quickly
NIST SP 800-171 Rev. 2 and Rev. 3 (03.15.01)	Policy and procedure documentation for contractor systems handling CUI
FISMA § 3554 and OMB A-130	Agencywide policy and procedures the statute requires
IG FISMA maturity, Level 2	Formalized, documented policies and procedures
NIST SP 800-37 Rev. 2	Artifacts used in the Prepare, Select and Implement steps and examined at Assess
HIPAA, 45 CFR § 164.316	Documentation overlay for health agencies

The policy suite is not the system security plan. The SSP (NIST SP 800-18) describes how each control is implemented on a specific system and cites the policies; this service writes the policies it cites. Keeping the two in separate scopes prevents the most common drift in this work.

Accurate	Not accurate
Assessor-ready policy and procedure documentation aligned to 800-53 Rev. 5, mapped control by control with a traceability matrix	Makes the agency compliant
Closes documentation findings and prepares the artifacts examined during assessment	ATO-ready or assessment-proof
Evidence that supports the authorization package	Delivers or accelerates the ATO

How an Engagement Runs

Phase	Standalone sprint	What happens
Kickoff and collection	Week 1	Existing policies, org chart, system inventory, latest findings and the directives template collected
Gap assessment	Weeks 1–2	Gap report and drafting plan; interviews scheduled by family cluster
Drafting waves	Weeks 2–6	Policies and SOPs drafted cluster by cluster; each wave goes to review as it is finished
Adjudication	Weeks 5–9	Two capped rounds; every comment dispositioned in writing
Finalization and handoff	Weeks 9–10	Signature-ready drafts, traceability matrix, governance charter, review calendar and briefing

As a bundled workstream inside an authorization or RMF engagement, the same work runs in 3 to 6 weeks in parallel with SSP work, because collection and interviews are shared with the parent effort. Duration scales with families, systems and reviewers, not with agency headcount.

What the Agency Provides

- A named adjudicator with authority to disposition comments.
- Subject matter experts for about 2 to 3 hours per family cluster.
- Review turnaround of five business days or less per round, with schedule relief written into the statement of work when it runs longer.
- The existing policy stack, org chart, system inventory and most recent assessment or IG findings at kickoff.
- The directives template and any style or 508 requirements in week one.

Acceptance is at delivery of the signature-ready draft. Formal issuance is an inherently governmental act and runs through the agency's directives process on its own schedule; tying acceptance to issuance would make the contract wait on the agency's legal and records review.

What Is Not Included

Included	Separate work
Policies the SSP cites	SSP authorship
Documentation findings closed in the suite	Building or managing the POA&M
Procedures for how controls are operated	Implementing or configuring the controls
Documents written to survive assessment	Conducting the assessment
Incident response and awareness training policies	The operational incident response plan, exercises and training courseware
Signature-ready drafts	Issuance through the directives process

How Avalon Staffs It

Avalon takes one engagement at a time and works on unclassified systems only. The delivery footprint is small: a senior policy lead at 60 to 80 percent who drafts and runs adjudication, a technical subject matter expert at 10 to 20 percent who checks that procedures match the tools, and part-time project management. Avalon has no past

federal engagements under this service, and it cites no credential, clearance or contract that is not current and verifiable.

Requirement	How it is handled
Senior author	A named lead and a named backup whose certifications and investigation level match the agency's requirements, listed in the proposal
Larger scopes	Additional authors or subject matter experts named in the proposal, hired or subcontracted, as a condition of the engagement
CUI received	No CUI accepted before a contract with safeguarding terms; work on government-furnished systems, or a current NIST SP 800-171 self-assessment and SPRS entry, as a condition of any engagement that sends Avalon CUI
Section 508	Documents produced to the agency's 508 and template requirements, stated as an acceptance criterion
Insurance	Coverage the contract requires, in place before award
Data rights	Delivered documents belong to the government; Avalon's preexisting methods stay Avalon's, stated in the proposal

Pricing and How to Buy

Shape	Market-norm range
Bundled workstream inside an A&A, RMF or readiness engagement	\$15K–\$40K increment, typically 10–20% of the parent
Standalone sprint (full family suite plus procedures)	\$45K–\$90K
Gap-and-refresh sprint (existing suite to the current revision)	\$20K–\$40K
Per document, where the agency prefers it	\$1.5K–\$5K per tailored policy; procedures comparable

The default is firm fixed price with an enumerated document list, two adjudication rounds included and additional rounds at a fixed per-round price agreed in advance. Labor-hour terms fit when the work is delivered inside an existing support contract. This is O&M-funded sustainment work, which makes July through September the natural buying window.

Every shape fits 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. Documentation bundled into a prime's authorization or RMF task order can be subcontracted to Avalon. Avalon does not hold a GSA Schedule or a governmentwide contract today.

A single-family pilot, one policy and its procedure priced per document with written acceptance criteria, is a reasonable first step for an agency that wants to see the method before committing to a suite.

Illustration: Sizing a Dash-One Sprint

The figures below are a planning illustration for one moderate-impact system, not a quote and not a result from any engagement. The sizing runs from the gap report: count the -1 controls by status, assign hours per document by gap type, then let lead capacity and review turnaround set the schedule.

Status of the -1 control	Families	Lead drafting hours each
Missing: no policy exists	3	9
Boilerplate: template never tailored (rewrite)	7	7
Stale: written to Rev. 4 (refresh)	6	4
Current: verify and map only	2	1
Role-assigned SOPs	7	6

PM-1 and PT-1 are treated as inherited from agency-level documents in this illustration, leaving 18 families at the system level. That gives 23 priced documents: 16 policies rewritten or refreshed and 7 SOPs. Interviews run across six family clusters.

Drafting wave	Families	Documents	Hours	Weeks
Wave 1	AC, IA, PS, AU, SI, RA	9	57	2–4
Wave 2	CM, MA, SA, SR, SC, MP, PE	8	58	4–6
Wave 3	CP, IR, AT, PL, CA	6	29	6

Work	Hours
Kickoff, collection and gap assessment	30
Practice-capture interviews (lead)	24
Drafting policies and SOPs	144
Traceability matrix, template and 508 pass	24
Two adjudication rounds	36
Governance charter, calendar and handoff	16
Lead total	274
Technical SME	47
Project management	28
Total	349

The lead carries about 6.8 FTE-weeks of work over 10 weeks, an average of 68 percent, and the SME about 12 percent. At an assumed blended rate of \$175 an hour, used only to check the effort, the work prices at \$62K fixed. That sits inside the \$45K–\$90K sprint band and works out to about \$2.7K per document, inside the \$1.5K–\$5K per-document range. Each round beyond the two included is priced at \$4K.

Reviewers Set the Critical Path

Review turnaround	2 rounds	3 rounds	4 rounds
5 business days	Week 10, \$62K	Week 12, \$66K	Week 14, \$70K
10 business days	Week 12, \$62K	Week 15, \$66K	Week 18, \$70K
15 business days	Week 14, \$62K	Week 18, \$66K	Week 22, \$70K

With five-day reviews and two rounds, handoff lands in week 10. Ten-day reviews push it to week 12 and fifteen-day reviews to week 14, with no change in the work or the price. Four rounds at five days end in week 14 and add \$8K. The slowest combination, fifteen-day reviews and four rounds, runs to week 22. Drafting speed barely moves the finish date; reviewer turnaround and round count do. That is why the five-day turnaround, the named adjudicator and the round cap belong in the statement of work.

If the Suite Only Needs a Refresh

If the gap report shows an existing Rev. 4 suite that is accurate but out of date, the same method sizes a lighter job: 12 policies refreshed, no new SOPs and shorter interviews. That comes to about 194 hours over 8 weeks and \$35K fixed, inside the \$20K–\$40K gap-and-refresh band at about \$2.9K per document.

Common Pitfalls

Pitfall	How to avoid it
Acceptance tied to issuance	Accept at the signature-ready draft; price issuance support separately if the agency wants it
Unlimited review rounds	Two rounds included, more at a fixed per-round price agreed in advance
Drift into SSP authoring	Separate scopes; the suite is what the SSP cites
Template shortcuts	Keep the interviews; shrink the family count instead
Families added mid-stream	An enumerated document list; additions by change order
Inconsistent pricing	The bundled increment matches the standalone math, so the same work never carries two prices
Compliance overselling	Use the accurate language in Section 5 in the proposal, the contract and every deliverable

Conclusion and Next Step

Dash-one findings are among the most fixable in an assessment. The controls are already operating in most cases; what is missing is a current, tailored description of how, who owns it and when it gets reviewed. Writing that down accurately takes interviews, traceability and a disciplined review process, not a larger template library.

The natural first step is the gap assessment that opens a sprint: a count of every -1 control by status, the drafting plan it implies, and a fixed price under the simplified acquisition threshold. Avalon drafts; the agency adjudicates, signs and issues; the Authorizing Official decides. To discuss a sprint or a single-family pilot, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

-1 control

The first control in each NIST SP 800-53 family (AC-1, AU-1 and so on), covering policy and procedures. PM-1 instead covers the information security program plan.

Adjudication

Collecting reviewer comments and recording a written disposition for each one.

BOD

A CISA Binding Operational Directive, mandatory for federal civilian executive branch agencies.

CSRMC

DoD's Cybersecurity Risk Management Construct, announced September 24, 2025.

CUI

Controlled Unclassified Information.

M-26-14

OMB memorandum (May 2026) that replaced M-21-31 with a risk-based logging model.

SOP

Standard operating procedure: step-level, role-assigned instructions.

Traceability matrix

A spreadsheet mapping each policy statement and procedure step to the control and assessment objective it supports.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Families in scope	18 (PM-1 and PT-1 inherited)	Planning assumption
Gap mix	3 missing, 7 boilerplate, 6 stale, 2 current	Planning assumption
Hours per document	Missing 9; boilerplate 7; stale 4; current 1; SOP 6	Planning assumption
Drafting capacity	32 lead hours a week; half in week 2	Lead at 80% during drafting
Review cycle	Turnaround plus one week to disposition and revise, per round	Planning assumption
Extra round	22 hours, \$4K	Disposition per document plus meeting
Price check	\$62K fixed; \$175 an hour blended for the effort check	Inside the \$45K–\$90K sprint band

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 800-53A Rev. 5, Assessing Security and Privacy Controls*
<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>
3. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework*
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
4. **National Institute of Standards and Technology**, *SP 800-171 Rev. 3, Protecting Controlled Unclassified Information*
<https://csrc.nist.gov/pubs/sp/800/171/r3/final>

5. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource*
<https://www.whitehouse.gov/omb/information-for-agencies/circulars/>
6. **Cybersecurity and Infrastructure Security Agency**, *Cybersecurity Directives (BOD 26-02, BOD 26-04)*
<https://www.cisa.gov/news-events/directives>
7. **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>
8. **FedRAMP**, *FedRAMP program site*
<https://www.fedramp.gov/>
9. **DoD Chief Information Officer**, *Cybersecurity Maturity Model Certification*
<https://dodcio.defense.gov/CMMC/>
10. **U.S. Department of Health and Human Services**, *HIPAA Security Rule*
<https://www.hhs.gov/hipaa/for-professionals/security/index.html>
11. **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/>