



Securing Tomorrow's Missions Today.



## **Authorization as an Engineering Practice: RMF Integration for Federal Systems**

---

NIST Risk Management Framework (RMF) Implementation: controls engineered in, evidence generated by the pipeline, and an authorization record that stays current.

[AvalonTechServices.com](https://AvalonTechServices.com)

[contact@AvalonTechServices.com](mailto:contact@AvalonTechServices.com)

|                                                                                       |           |
|---------------------------------------------------------------------------------------|-----------|
| <b>Executive Summary</b>                                                              | <b>2</b>  |
| <b>Why Authorizations Stall</b>                                                       | <b>3</b>  |
| What Triggers the Work                                                                | 3         |
| How the Need Sounds                                                                   | 4         |
| <b>Where RMF Is Heading: Ongoing Authorization, cATO and CSRMC</b>                    | <b>4</b>  |
| <b>What RMF Integration Covers</b>                                                    | <b>6</b>  |
| <b>Deliverables and Boundaries</b>                                                    | <b>7</b>  |
| What the Service Does Not Include                                                     | 8         |
| <b>How an Engagement Runs</b>                                                         | <b>8</b>  |
| The Avalon Team                                                                       | 10        |
| What the Agency Provides                                                              | 10        |
| <b>Evidence as Code: Pipeline Gates, Compliance-as-Code and Continuous Monitoring</b> | <b>11</b> |
| Pipeline Control Gates                                                                | 11        |
| Compliance-as-Code Profiles                                                           | 11        |
| Continuous Monitoring                                                                 | 11        |
| <b>What the Service Supports, and What It Does Not</b>                                | <b>12</b> |
| <b>An Illustrative Engagement</b>                                                     | <b>13</b> |
| What the Illustration Shows                                                           | 14        |
| <b>Pricing and Contracting</b>                                                        | <b>15</b> |
| How the Work Is Bought                                                                | 15        |
| <b>Risks and How the SOW Contains Them</b>                                            | <b>16</b> |
| <b>Conclusion and Next Step</b>                                                       | <b>16</b> |
| <b>Appendices</b>                                                                     | <b>17</b> |
| Appendix A: Glossary                                                                  | 17        |
| Appendix B: Control Map                                                               | 18        |
| Appendix C: Illustration Assumptions                                                  | 19        |
| Appendix D: References                                                                | 20        |

## Executive Summary

Every federal information system must be authorized before it operates, and the NIST Risk Management Framework (RMF) is the process that gets it there. At most agencies that process still runs as an end-of-lifecycle documentation exercise. Industry reporting puts a traditional authorization at 12 to 18 months. Packages go stale within a quarter of signature, and new capability waits in a queue behind paperwork while the system it was meant to replace keeps running.

The framework is not the problem. OMB Circular A-130 already expects ongoing authorization rather than a signature every three years, and DoD's continuous authorization (cATO) pathway and its Cybersecurity Risk Management Construct (CSRMC), announced in September 2025, push further toward automation, continuous monitoring and reciprocity. What most programs lack is the engineering underneath: controls designed in from categorization forward, evidence produced by the tools that build and run the system, and a governance record that reflects the system as it actually is.

This paper is written for agency CISOs and ISSMs, the system program managers whose deployments are waiting on an authorization, and the contracting officers who buy the work. It describes Avalon Technology Services' RMF Integration service, which wires the framework into how an agency builds and operates a system:

- **Security engineered in.** Categorization, a tailored control baseline, and an inheritance architecture set before implementation, not reconstructed after it.
- **Evidence as code.** Pipeline control gates, compliance-as-code profiles and continuous monitoring feeds that keep control evidence current without a manual data call.
- **A record that stays current.** The authorization record in eMASS, Xacta or CSAM structured so it matches the deployed system every day, not just the day of assessment.

Two boundaries matter. Avalon does not assess the system: an independent assessor does. And Avalon does not grant, promise or time the authorization: that decision always stays with the government Authorizing Official (AO). The service removes the delays a contractor can control, such as package quality, stale evidence and assessment rework, and positions the system for independent assessment and the authorization decision.

The entry point is a fixed-price readiness assessment of \$15K to \$35K. Section 9 walks through an illustrative engagement for one Moderate-baseline system costing \$185K.

The engagement pays for itself if it removes about 3.7 months of delay on its own, sooner when recurring evidence labor falls, and the same section shows the case where it does not pay back.

## Why Authorizations Stall

Authorization delays rarely come from a single cause. They come from the way RMF work is sequenced and staffed.

| Cause                                | How it shows up                                                                                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RMF runs at the end of the lifecycle | Categorization and control selection happen after the system is built, so implementation statements describe intent rather than configuration and assessors find the gap. |
| Evidence is collected by hand        | ISSOs spend their weeks assembling screenshots and scan exports for each assessment and each data call. The evidence is stale by the time it is reviewed.                 |
| Packages drift                       | The system changes weekly; the System Security Plan changes at reauthorization. Within a quarter of signature, the package no longer describes the system.                |
| Inheritance is undocumented          | Controls inherited from a cloud provider or enterprise service are asserted rather than mapped, and the AO will not accept them without a customer responsibility matrix. |
| The record is disorganized           | Control mappings, test results and POA&Ms in the governance platform are incomplete or inconsistent, so every review starts with cleanup.                                 |
| Access takes weeks                   | Accounts for eMASS and similar platforms require government sponsorship and training. Engagements that do not start access requests at kickoff lose their first month.    |

## What Triggers the Work

- A new system or major change that cannot deploy until it is authorized, with a date the program cannot move.
- A reauthorization cycle approaching on a package nobody trusts.

- IG or FISMA findings on continuous monitoring, POA&M management or authorization currency.
- Leadership direction to pursue ongoing authorization or cATO, with no plan for what it takes.
- A move to a cloud platform, where inherited controls must be mapped before the new boundary is authorized.
- Loss of the one person who understood the package.

## **How the Need Sounds**

Each of these points to the same service: "Our packages are shelfware." "The last ATO took fourteen months." "We rewrite the SSP from scratch every cycle." "Our ISSOs spend their whole week inside eMASS." "The AO won't accept our inherited controls." "We can't push code until the reauthorization clears." "Leadership wants cATO and nobody can say what that takes."

## **Where RMF Is Heading: Ongoing Authorization, cATO and CSRMC**

The policy direction has been consistent for a decade, and it has accelerated since 2022. Every step moves authorization away from a periodic document review and toward continuous, evidence-based risk management.

| Development                                                                               | What it means for a program office                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NIST SP 800-37 Rev. 2 (2018)                                                              | Seven steps, starting with Prepare, and explicit support for ongoing authorization based on continuous monitoring                                                                                                                                                         |
| OMB Circular A-130 (2016)                                                                 | Requires agencies to use the RMF and moves them toward ongoing authorization instead of fixed three-year cycles                                                                                                                                                           |
| DoD cATO memorandum (February 2022) and 2024 evaluation criteria and implementation guide | A path to continuous authorization for DevSecOps programs that demonstrate three competencies: continuous monitoring of RMF controls, active cyber defense, and use of an approved DevSecOps reference design                                                             |
| DoDI 8510.01 (July 2024 reissue)                                                          | DoD's RMF implementation, with eMASS as the record of authorization and reciprocity expectations                                                                                                                                                                          |
| DoD Cybersecurity Risk Management Construct (announced September 24, 2025)                | Named as the successor to RMF across DoD. Its ten tenets include automation, continuous monitoring and ATO, DevSecOps, enterprise services and inheritance, and reciprocity. RMF processes, DoDI 8510.01 and eMASS remain in use while implementation guidance is issued. |
| FedRAMP Consolidated Rules (launched June 25, 2026)                                       | A cloud-provider program, not agency authorization, but it resets expectations: machine-readable evidence and continuous validation, mandatory from January 1, 2027                                                                                                       |

The common thread is that an authorization decision should rest on evidence the system produces continuously. Whatever DoD's construct is finally called in its implementing instruction, a program that has engineered its controls, automated its evidence and structured its record will be ready for it. A program still assembling screenshots will not.

## What RMF Integration Covers

A full engagement covers nine activity areas. The specificity is deliberate: much of the market sells RMF support as document-production hours, and this service sells an engineered practice the agency keeps.

| # | Activity area                               | What Avalon does                                                                                                                                                                                   |
|---|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Authorization posture assessment            | Review the current package, governance record, inheritance, monitoring and pipeline; measure the gap to ongoing authorization                                                                      |
| 2 | Categorization and baseline tailoring       | Validate categorization (FIPS 199, SP 800-60; CNSSI 1253 for national security systems); select and tailor the SP 800-53B baseline; document organization-defined parameters and overlay rationale |
| 3 | Inheritance and common control architecture | Map inherited, hybrid and system-specific controls; build the customer responsibility matrix for controls inherited from FedRAMP-certified cloud services and enterprise providers                 |
| 4 | Control implementation engineering          | Write implementation statements that match actual configuration, and specify the engineering changes where they do not                                                                             |
| 5 | Pipeline and compliance-as-code             | Design control gates in the CI/CD pipeline; build SCAP, OpenSCAP and InSpec profiles; structure artifacts for OSCAL where the platform supports it                                                 |
| 6 | Governance platform integration             | Structure the authorization record in eMASS, Xacta, CSAM, ServiceNow IRM or Archer: control mapping, test result import, POA&M workflow, inheritance, artifacts                                    |
| 7 | Continuous monitoring (ISCM)                | Design the monitoring strategy per SP 800-137: frequency per control, metrics, data feeds, and reporting cadence to the AO                                                                         |
| 8 | Continuous authorization readiness (DoD)    | Map evidence to the DoD cATO evaluation criteria and the three competencies                                                                                                                        |

| # | Activity area      | What Avalon does                                                                                            |
|---|--------------------|-------------------------------------------------------------------------------------------------------------|
| 9 | Knowledge transfer | Runbooks, standard procedures, training and a declining-involvement handoff so agency staff run the process |

## Deliverables and Boundaries

| Deliverable                                            | Format                                           | RMF step                   |
|--------------------------------------------------------|--------------------------------------------------|----------------------------|
| Authorization posture assessment report                | Report and executive briefing                    | Prepare                    |
| RMF integration roadmap, prioritized and costed        | Report                                           | Prepare                    |
| Categorization package                                 | Worksheets and governance record entries         | Categorize                 |
| Tailored control baseline with parameter workbook      | Workbook and governance record                   | Select                     |
| Inheritance matrix and customer responsibility mapping | Workbook and governance record                   | Select, Implement          |
| Control implementation statements                      | Native governance records; OSCAL where supported | Implement                  |
| Pipeline gate designs and compliance-as-code profiles  | Code repository and design document              | Implement                  |
| Continuous monitoring strategy and plan                | Report and configured tool integrations          | Monitor                    |
| cATO readiness evidence map (DoD)                      | Mapped to the DoD evaluation criteria            | Monitor, Authorize support |
| Runbooks, procedures and training                      | Wiki or documents, plus live sessions            | All                        |

## What the Service Does Not Include

| Excluded                                     | Where it belongs                                                                                                                  |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Independent security control assessment      | An independent assessor. Avalon does not assess a system it prepared, to avoid an organizational conflict of interest.            |
| The authorization decision                   | The government Authorizing Official, always                                                                                       |
| Standalone SSP or POA&M production           | Separate Avalon services. Here they are work products inside the engagement.                                                      |
| Remediation of every finding                 | The agency, or Avalon's Remediation & Patch Management service by change order. Hands-on remediation hours are capped in the SOW. |
| Penetration testing                          | A separate assessment service                                                                                                     |
| Enterprise identity or zero trust deployment | Separate services. This engagement integrates them and maps them to controls.                                                     |
| Indefinite ISSO staffing                     | A separately scoped support arrangement. The engagement includes a bounded transition only.                                       |

The language matters as much as the scope. A proposal or status brief should say the service "engineers and documents the control baseline," "establishes continuous monitoring that supports CA-7 and the agency's monitoring strategy," and "positions the system for independent assessment and the authorization decision." It should never say the service delivers an ATO, guarantees an assessment result, or provides a "cATO certification." Continuous authorization is not a certification; it is an authorization state the AO grants and can revoke.

## How an Engagement Runs

A single-system engagement at the Moderate baseline, in an unclassified or CUI environment, runs in five phases.

| Phase                                | Duration   | Core activities                                                                                                                                 | Exit criteria                                             |
|--------------------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 0. Kickoff and access                | 1–2 weeks  | Account and tool access requested, documents collected, stakeholder map, kickoff with system owner, ISSM and AO representative                  | Access requests submitted; document inventory complete    |
| 1. Posture assessment and roadmap    | 3–5 weeks  | Package and record review, interviews, tooling and pipeline review, gap analysis against the SP 800-53 baseline and, for DoD, the cATO criteria | Assessment report and roadmap accepted                    |
| 2. Framework structuring             | 4–8 weeks  | Categorization validation, baseline tailoring and parameters, inheritance architecture, governance record restructure                           | Baseline and record architecture approved                 |
| 3. Implementation and automation     | 8–16 weeks | Control implementation engineering, pipeline gates, compliance-as-code, evidence automation, monitoring tool integration                        | Controls implemented and evidenced; monitoring feeds live |
| 4. Operationalization and transition | 4–6 weeks  | Runbooks, training, an assessment-readiness dry run, declining-involvement handoff                                                              | Agency staff run the process independently                |

A single Moderate system typically takes four to eight months. A program-level or portfolio engagement takes six to twelve. Duration grows with the number of systems, the classification level, the condition of the governance record, and how much of the environment is legacy rather than pipeline-delivered. Phases 0 and 1 together form the readiness assessment, which can be bought on its own.

## The Avalon Team

| Role                                       | Involvement                              | Responsibility                                                                                  |
|--------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------|
| Engagement lead / senior security engineer | 0.5–1.0 FTE, full engagement             | Technical direction, control implementation engineering, interface with the AO's representative |
| RMF / compliance specialist                | 0.5–1.0 FTE, phases 1–4                  | Categorization, tailoring, governance record work, documentation quality                        |
| DevSecOps engineer                         | 0.5–1.0 FTE, phase 3 plus phase 1 review | Pipeline gates, compliance-as-code, evidence automation                                         |
| Project manager                            | 0.25 FTE                                 | Schedule, agency-side dependencies, reporting                                                   |

The team is two to four people, weighted toward senior engineers. It is deliberately not a staffing model.

## What the Agency Provides

These go into the SOW as conditions, because schedule slippage on this work most often traces to access, not to the technical tasks:

- System owner and ISSO time of four to eight hours a week, and a designated ISSM with decision authority.
- Governance platform accounts for Avalon staff. eMASS access requires government sponsorship and completed training and can take several weeks, so requests start at kickoff.
- Administrative or paired-engineer access to the systems and pipeline in scope, and access to scanner output.
- Prior packages, network diagrams and assessment reports.
- Scheduled touchpoints with the AO or the AO's designated representative at each phase gate.

## **Evidence as Code: Pipeline Gates, Compliance-as-Code and Continuous Monitoring**

The technical core of the service is moving evidence production from people to systems. Three layers do the work.

### **Pipeline Control Gates**

Every change that reaches production passes through the build pipeline, which makes the pipeline the natural place to check and record controls. Gates run configuration scans against the applicable DISA STIGs or agency baselines, dependency and image scanning, and policy checks on infrastructure-as-code templates. A failed gate stops the change or opens a tracked exception. A passed gate writes a dated, attributable result to the evidence store. Configuration management controls (CM-2, CM-3, CM-6) stop being a narrative in the SSP and become a record of every change.

### **Compliance-as-Code Profiles**

Control checks are written as code: SCAP content and the SCAP Compliance Checker where DoD requires them, OpenSCAP for operating system baselines, and InSpec profiles for application and cloud configuration. Each check is tied to the control it evidences, so an assessor can trace a control to the test that proves it and to the date it last passed. Where the governance platform accepts it, results and implementation statements are structured in OSCAL, NIST's machine-readable format for security plans, assessment results and POA&Ms.

### **Continuous Monitoring**

The monitoring strategy, written per SP 800-137, sets a frequency for each control, the metric that shows it is working, the data feed that supplies the metric, and the cadence of reporting to the AO. Vulnerability scanners, configuration monitoring and pipeline results feed the governance record directly. New findings open POA&M items with owners and dates; closed findings close them. The result supports CA-7 and gives the AO a current view of risk rather than a snapshot that ages from the day it is taken.

None of this replaces judgment. Some controls, such as policy, training and contingency planning, will always need people to evidence them. The goal is to automate the evidence that can be automated, so that ISSOs spend their time on the risk decisions that cannot.

## What the Service Supports, and What It Does Not

| Framework or authority                 | Relationship                            | What the service addresses                                                                                                           |
|----------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| FISMA (44 U.S.C. § 3551 et seq.)       | Statutory driver                        | Risk assessment, security planning, periodic testing, continuous monitoring and remediation processes                                |
| OMB Circular A-130                     | Mandate to use the RMF                  | The move from periodic reauthorization to ongoing authorization                                                                      |
| NIST SP 800-37 Rev. 2                  | The process itself                      | Operationalizes Prepare, Categorize, Select, Implement and Monitor; prepares the system for Assess and Authorize                     |
| NIST SP 800-53 Rev. 5                  | Control catalog                         | Directly supports CA-2, CA-5, CA-6, CA-7, PL-2, PM-9, PM-10, PM-31, RA-3, RA-5, RA-7, CM-2, CM-3 and CM-6 (Appendix B)               |
| NIST SP 800-137                        | Continuous monitoring                   | The monitoring strategy, metrics and program                                                                                         |
| DoDI 8510.01 and the DoD cATO criteria | DoD implementation                      | eMASS record structure, reciprocity posture, and the evidence base for continuous authorization                                      |
| DoD CSRMC                              | DoD successor construct                 | The same automation, monitoring, inheritance and reciprocity work, ready for the implementing guidance                               |
| ICD 503                                | Intelligence Community parallel process | Same integration logic on Xacta; requires cleared staff and is outside Avalon's current offer                                        |
| FedRAMP                                | Adjacent                                | Inherited controls from FedRAMP-certified cloud services, mapped in the agency's package. Avalon does not authorize cloud providers. |

| Framework or authority   | Relationship    | What the service addresses                                   |
|--------------------------|-----------------|--------------------------------------------------------------|
| NIST SP 800-171 and CMMC | Different scope | Contractor CUI environments, not agency system authorization |

## An Illustrative Engagement

The figures below are a planning illustration for one representative system, not a quote and not a result from any engagement. They do not assume that the engagement shortens authorization by any fixed percentage, because no vendor controls the assessment schedule or the AO's decision. Instead, the illustration asks a narrower question: how much vendor-controllable delay does the engagement have to remove to pay for itself?

The agency is replacing a legacy system with a new Moderate-baseline system. Until the new system is authorized, the legacy system keeps running at \$50K a month. Agency and support staff spend 1,600 hours a year collecting evidence and maintaining the package by hand, at a blended \$150 an hour. The engagement costs \$185K: a \$25K readiness assessment followed by a \$160K fixed-price integration. Automated evidence feeds go live in month 7.

| Scenario (three years)         | Labor shifted to automation | Delay removed | Gross value | Net of cost | Payback month      |
|--------------------------------|-----------------------------|---------------|-------------|-------------|--------------------|
| Base case: 40% labor, 2 months | \$96K a year                | 2 months      | \$340K      | \$155K      | 17                 |
| 40% labor, 4 months            | \$96K a year                | 4 months      | \$440K      | \$255K      | 8                  |
| 40% labor, 0 months            | \$96K a year                | 0 months      | \$240K      | \$55K       | 30                 |
| 20% labor, 2 months            | \$48K a year                | 2 months      | \$220K      | \$35K       | 28                 |
| 20% labor, 4 months            | \$48K a year                | 4 months      | \$320K      | \$135K      | 8                  |
| 20% labor, 0 months            | \$48K a year                | 0 months      | \$120K      | -\$65K      | Not within 3 years |

Discounted at the 1.1% three-year real rate in OMB Circular A-94's 2026 Appendix C, the base case is worth \$150K to the agency over three years and pays back in month 17.

### What the Illustration Shows

- **Delay is the larger lever.** At \$50K a month, removing about 3.7 months of delay covers the whole engagement without counting any labor savings.
- **Labor savings are slower but recurring.** They continue after the engagement ends, as long as the agency keeps the pipeline gates and monitoring feeds running.
- **It does not always pay.** With little manual labor to shift and no delay to remove, the engagement does not pay back within three years. An agency in that position should buy the readiness assessment, which shows whether the delay and labor exist, and may reasonably stop there.

*The agency's own figures replace every assumption here during the readiness assessment. Appendix C lists each input.*

## Pricing and Contracting

| Scope                                  | Description                                                      | Typical firm fixed price |
|----------------------------------------|------------------------------------------------------------------|--------------------------|
| Readiness assessment (entry offer)     | Posture assessment and roadmap only (phases 0–1)                 | \$15K–\$35K              |
| Single system, Moderate baseline       | Phases 0–4, one system, unclassified or CUI                      | \$75K–\$250K             |
| Portfolio or program-level integration | Multiple systems, enterprise record restructure, cATO enablement | \$250K–\$1.2M            |

*These are market-norm planning ranges, validated against the specific system and solicitation before any figure appears in a proposal.*

Integration phases are priced firm fixed price with bounded deliverables and named systems, so the risk of overrun sits with Avalon rather than the agency. Labor-hour rates, where a solicitation requires them, fall within market norms for the category: roughly \$140 to \$190 an hour for an RMF specialist and \$150 to \$230 for senior security and DevSecOps engineers, fully burdened and unclassified. Performance-based pricing does not fit compliance work and is not offered.

## How the Work Is Bought

The readiness assessment and most single-system engagements fall under the simplified acquisition threshold, which rose to \$350,000 on October 1, 2025, so they can be bought as open-market purchases. Larger scopes can be ordered through GSA's Multiple Award Schedule (IT Professional Services and Highly Adaptive Cybersecurity Services), OASIS+, or SeaPort-NxG for Navy and Marine Corps customers. The readiness assessment also fits fourth-quarter O&M money, because it produces a roadmap the next fiscal year's budget can fund.

## Risks and How the SOW Contains Them

| Risk                                                       | Likelihood | Impact | Containment                                                                                                  |
|------------------------------------------------------------|------------|--------|--------------------------------------------------------------------------------------------------------------|
| Access provisioning delays the start                       | High       | High   | Access requests at kickoff; the schedule runs from access grant; agency obligations written into the SOW     |
| "Integration" turns into indefinite ISSO staffing          | Medium     | High   | Systems named by record ID; a time-boxed transition; ongoing support scoped separately                       |
| Implementation becomes remediation of every finding        | Medium     | Medium | Hands-on remediation hours capped; overflow by change order                                                  |
| One system becomes the whole enclave                       | Medium     | Medium | A change-control trigger on any request touching a system not listed                                         |
| Compliance oversell                                        | Low        | High   | Approved language only; no promised timelines or outcomes that belong to the assessor or AO                  |
| Policy change mid-engagement (for example, CSRMC guidance) | Medium     | Low    | Evidence built to the underlying controls, which carry across constructs; roadmap updated at each phase gate |

## Conclusion and Next Step

Authorization will keep moving toward continuous evidence, whether through A-130's ongoing authorization, DoD's cATO pathway, or the construct that replaces RMF across DoD. Programs that treat it as a documentation event will keep paying for delay and stale packages. Programs that engineer their controls, automate their evidence and keep their record current will be ready for whatever the next instruction requires.

The first step is the fixed-price readiness assessment: three to seven weeks, \$15K to \$35K, producing a costed roadmap and a clear answer on whether a full integration is worth buying. Avalon runs one engagement at a time, in unclassified and CUI

environments, led by senior engineers. Avalon is a small business without prior federal contracts under this service, and says so; the fixed-price, deliverable-based structure is built to keep the agency's exposure small. To discuss a readiness assessment, contact Avalon Technology Services at [contact@AvalonTechServices.com](mailto:contact@AvalonTechServices.com).

## Appendices

### Appendix A: Glossary

**AO: Authorizing Official**

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

**AODR: AO Designated Representative**

The official who acts for the AO in day-to-day authorization matters.

**cATO: Continuous Authorization to Operate**

An ongoing authorization state for DoD systems that demonstrate continuous monitoring, active cyber defense and DevSecOps delivery. It is granted by the AO and can be revoked; it is not a certification.

**CRM: Customer Responsibility Matrix**

The mapping of which controls a system inherits from a provider and which it must implement itself.

**CSAM**

A governance platform used by many civilian agencies to manage authorization records.

**CSRMC: Cybersecurity Risk Management Construct**

DoD's successor to RMF, announced September 24, 2025.

**eMASS**

DoD's system of record for RMF authorization packages.

**ISCM: Information Security Continuous Monitoring**

The ongoing monitoring program defined in NIST SP 800-137.

**ISSM / ISSO**

Information System Security Manager and Officer: the staff responsible for a system's security program and its day-to-day security.

**ODP: Organization-Defined Parameter**

A value in an SP 800-53 control that the organization sets, such as a frequency or threshold.

**OSCAL**

NIST's Open Security Controls Assessment Language, a machine-readable format for security plans, assessments and POA&Ms.

**POA&M: Plan of Action and Milestones**

The tracked list of known weaknesses and the plan and dates for correcting them.

**SCA: Security Control Assessor**

The independent party that assesses whether controls are implemented correctly and working as intended.

**SSP: System Security Plan**

The document that describes a system's boundary, environment and control implementation.

**Appendix B: Control Map**

The NIST SP 800-53 Rev. 5 controls the service most directly supports, and the evidence an engagement produces for each.

| Control            | Name                                                      | Evidence the engagement produces                                                           |
|--------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------|
| CA-2               | Control assessments                                       | An assessment-ready package and a readiness dry run (the assessment itself is independent) |
| CA-5               | Plan of action and milestones                             | A POA&M workflow fed by scanner and pipeline results                                       |
| CA-6               | Authorization                                             | A current record and evidence base for the AO's decision                                   |
| CA-7, CA-7(4)      | Continuous monitoring; risk monitoring                    | The monitoring strategy, metrics and live data feeds                                       |
| CM-2, CM-3, CM-6   | Baseline, change control, configuration settings          | Pipeline gate results and compliance-as-code scan history                                  |
| PL-2               | System security plan                                      | Implementation statements matched to actual configuration                                  |
| PM-9, PM-10, PM-31 | Risk strategy, authorization process, monitoring strategy | Organization-level process documentation and the monitoring strategy                       |
| RA-3, RA-5, RA-7   | Risk assessment, vulnerability monitoring, risk response  | Scanner integration and tracked risk responses                                             |

## Appendix C: Illustration Assumptions

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

| Assumption               | Value  | Basis                                      |
|--------------------------|--------|--------------------------------------------|
| Readiness assessment     | \$25K  | Inside the \$15K–\$35K tier                |
| Integration (phases 2–4) | \$160K | Inside the \$75K–\$250K single-system tier |

| Assumption                                         | Value                                                         | Basis                                                         |
|----------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------|
| Cost of each month the legacy system keeps running | \$50K                                                         | Planning assumption; replaced by the agency's own figure      |
| Manual evidence and package labor                  | 1,600 hours a year at \$150 an hour                           | Planning assumption; blended rate within market-norm ranges   |
| Share of that labor shifted to automation          | 20% or 40%                                                    | Planning assumption                                           |
| Months of delay removed                            | 0, 2 or 4                                                     | Planning assumption; no fixed percentage reduction is assumed |
| Timing                                             | Automation live in month 7; delay value in month 8            | Within the four-to-eight-month engagement                     |
| Discount rate                                      | 1.1% real, three-year                                         | OMB Circular A-94, Appendix C (2026)                          |
| Excluded                                           | Remediation labor, tool licenses, assessment costs, inflation | Outside the engagement or already budgeted                    |

## Appendix D: References

1. **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>
2. **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>
3. **National Institute of Standards and Technology**, *SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and*

*Organizations, September 2011*

<https://csrc.nist.gov/pubs/sp/800/137/final>

4. **National Institute of Standards and Technology**, *OSCAL: Open Security Controls Assessment Language*  
<https://pages.nist.gov/OSCAL/>
5. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource, 2016*  
<https://www.whitehouse.gov/omb/information-resources/guidance/circulars/>
6. **Office of Management and Budget**, *Circular A-94, Appendix C: Discount Rates (2026)*  
<https://www.whitehouse.gov/omb/information-resources/guidance/circulars/>
7. **Department of Defense**, *DoD Instruction 8510.01, Risk Management Framework for DoD Systems, July 2024*  
<https://www.esd.whs.mil/Directives/issuances/dodi/>
8. **Akin Gump**, *Department of Defense Launches CSRMC: A New Cybersecurity Risk Management Construct, October 2, 2025*  
<https://www.akingump.com/en/insights/alerts/department-of-defense-launches-csrmc-a-new-cybersecurity-risk-management-construct>
9. **Crowell & Moring**, *Time for a Change: FedRAMP Fundamentally Revamps Program With Consolidated Rules for 2026, July 7, 2026*  
<https://www.crowell.com/en/insights/client-alerts/time-for-a-change-fedramp-fundamentally-revamps-program-with-consolidated-rules-for-2026>
10. **FedTech Magazine**, *Continuous ATO and the Future of Federal IT Cloud Security, August 2026*  
<https://fedtechmagazine.com/article/2026/08/continuous-ato-and-future-federal-it-cloud-security-perfcon>
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/>