PANDORA CLOUD
UNPACKING COMPLEXITY

FedRAMP/NIST Readiness Checklist

NIST 800-53 Rev 5 control posture and DoD impact level scoping for SBIR companies, defense subcontractors, and SMBs pursuing federal authorization

A Pandora Cloud Buyer's Resource

May 2026

Pandora Cloud LLC
Women-Owned Small Business (WOSB) | AWS Advanced Partner
GSA MAS: 47QTCA24D00D3 | CAGE: 9JSG7 | UEI: R36GQ3N4XT63
Secret Facility Clearance | pandoracloud.net

About This Checklist

Federal authorization has become the dividing line between Small and Medium-sized Businesses (SMBs) that can compete for federal contracts and those that watch the opportunity pass. The Federal Risk and Authorization Management Program (FedRAMP) governs cloud authorizations for federal civilian agencies; the Department of Defense (DoD) Cloud Computing Security Requirements Guide (CC SRG) adds Impact Levels that govern Controlled Unclassified Information (CUI) and mission-critical workloads; the National Institute of Standards and Technology (NIST) 800-53 Rev 5 catalog underlies both. The combination of these three reference points is what most SMBs face when their first federal opportunity becomes real.

This checklist is for the Small Business Innovation Research (SBIR) companies preparing to transition from Phase II to Phase III, the defense subcontractors stepping up to direct primes, and the SMBs whose first federal opportunity has arrived faster than their compliance posture. It is structured around the actual sequence of decisions and artifacts that drive an Authorization to Operate (ATO) for a small team, written for a founder or technology lead rather than a federal compliance specialist, and designed to expose the gaps that most often add months to an authorization timeline.

Use the 36-item checklist to score your current readiness. Use the 6-month sprint plan to map your move from current state to assessment kickoff. Use the impact-level decision framework, common-findings reference, and Third-Party Assessment Organization (3PAO) selection guidance to make the higher-stakes decisions that shape your authorization path.

Reading time: 30 minutes to score yourself; 90 minutes to walk through it with the team. The cost-and-timeline sections reward a second read with your finance lead.

Why Federal Authorization Is the Wall Most SMBs Hit

Three shifts in the last twenty-four months explain why FedRAMP and NIST 800-53 Rev 5 have moved from "later" to "now" for SMBs targeting federal work.

1. Continuous Authorization to Operate (cATO) is replacing the calendar-based ATO model. Traditional Authorizations to Operate (ATOs) granted a one-to-three-year authorization and assumed re-authorization on a fixed schedule. That model is being deprecated across DoD program offices, civilian agencies, and Cybersecurity Maturity Model Certification (CMMC) pre-assessment workflows. SBIR companies and emerging primes that demonstrate continuous monitoring posture get faster initial authorizations and longer authorization windows. Teams still chasing one-time ATOs are increasingly out of step with where the market has moved.

2. NIST 800-53 Rev 5 superseded Rev 4 and the transition is mostly complete. FedRAMP officially moved to Rev 5 in 2023; agency-specific frameworks followed. Organizations whose System Security Plans (SSPs) and control matrices still reference Rev 4 baselines are being flagged as out of date, even when the underlying controls remain technically equivalent. Rev 5 also introduces the Supply Chain Risk Management (SR) control family and integrates privacy controls into the catalog rather than treating them as a separate overlay. The remap is operational work, not optional cleanup.

3. The SBIR-to-Phase-III gap has widened. Phase II grants are easier to win than they used to be; Phase III contracts are harder to bridge to without an authorized cloud environment. The companies bridging the gap successfully are the ones who built compliant infrastructure before the Phase II milestone, not after. The vendors who wait for a Phase III opportunity to start an ATO conversation typically miss the contract window the opportunity opens.

The companies moving through federal authorization in months and not years are not technically more advanced; they are operating against a different posture. They built the controls before the assessment. They mapped to NIST 800-53 Rev 5 from day one. They captured evidence as a side effect of normal work, not under deadline pressure. They treated authorization as a continuous condition, not a milestone.

How to Use This Checklist

Walk through the 36 items below with your team. For each item, mark one of:

- Implemented: the control is in place and you have evidence to show it.
- Partial: the control is partially in place; gaps exist.
- Missing: the control does not exist or has not been documented.

Count the implemented items. Use the scoring tiers at the end of this document to determine whether you are ready to engage a Third-Party Assessment Organization (3PAO) or still have foundational work to complete.

Save your scored checklist. Re-score quarterly so you can see whether your posture is strengthening, holding, or drifting between assessment cycles.

Section 1: Authorization Scope and System Boundary

The first artifact a 3PAO will ask for is your authorization boundary diagram. Most SBIR and SMB teams underscope the boundary on the first pass and over-include connected systems they cannot defend.

- [ ] Authorization boundary diagram drafted, showing all components within the boundary and the data flows that cross it.
- [ ] System characterization documented (system name, owner, function, categorization, FIPS 199 impact level).
- [ ] Federal Information Processing Standards (FIPS) 199 impact categorization completed for Confidentiality, Integrity, and Availability.
- [ ] External services and interconnections inventoried, with FedRAMP authorization status for each cloud dependency.
- [ ] Data flow diagram showing how CUI or sensitive federal data moves into, through, and out of the system.
- [ ] Authorization path selected (agency ATO, Joint Authorization Board provisional ATO, or FedRAMP Tailored Low Impact Software-as-a-Service (LI-SaaS)).

Section 2: NIST 800-53 Rev 5 Control Selection

Control selection is where most SBIR companies waste the first two months of their authorization sprint. The baselines are well-defined; the work is choosing the right one and mapping it honestly to your environment.

- [ ] Target baseline selected (Low Impact, Moderate Impact, or High Impact) with documented rationale.
- [ ] Control implementation summary drafted for every control in the selected baseline.
- [ ] Tailoring decisions documented for any controls being adjusted, with risk justification.
- [ ] Compensating controls documented where the baseline control cannot be implemented as written.
- [ ] Privacy controls (PT family) addressed if Personally Identifiable Information (PII) is in scope.
- [ ] Supply Chain Risk Management (SR family) controls implemented and documented, including vendor security review evidence.

Section 3: Continuous Monitoring and POA&M Discipline

FedRAMP authorization is not the finish line; it is the beginning of a continuous monitoring (ConMon) cadence. The teams that pass annual assessments cleanly are the ones whose ConMon discipline never let the posture drift.

- [ ] Vulnerability scanning configured for operating system, web application, and database layers, with monthly cadence.
- [ ] Plan of Action and Milestones (POA&M) tracking active for all open findings, with owners and target close dates.
- [ ] Significant change request process documented for major system changes that require Authorizing Official notification.
- [ ] Annual security assessment plan scoped, with 3PAO engagement confirmed for re-assessment cycles.
- [ ] Monthly ConMon deliverables process defined (scan results, POA&M updates, inventory updates).
- [ ] Continuous monitoring metrics reviewed at executive level at least quarterly.

Section 4: Identity, Access, and Audit Logging

Identity and Access Management (IAM) is the top-cited finding category in returned ATO packages across our defense and federal SMB practice. The fix is operational hygiene, not architecture.

- [ ] Multi-factor authentication (MFA) enforced for all privileged and remote access, using a Federal Information Processing Standards (FIPS) 140-validated module.
- [ ] Role-based access control aligned to least privilege, with documented role definitions.
- [ ] Privileged access reviewed monthly with documented justification and removal of unused privileges.

- [ ] Just-in-time access implemented for break-glass and emergency operations, with audit trail.
- [ ] Audit logging enabled across all in-scope systems with the log content required by NIST 800-53 AU controls.
- [ ] Log retention meets the longer of your authorization commitment and any contractual flowdown requirement.

Section 5: Supply Chain and FedRAMP-Authorized Services

Rev 5 made Supply Chain Risk Management a control family rather than an afterthought. Assessors increasingly trace cloud dependencies, third-party Software-as-a-Service (SaaS) tools, and subprocessor relationships to confirm the upstream posture matches your claimed authorization level.

- [ ] All cloud services in scope verified as FedRAMP authorized at the equivalent impact level (Low, Moderate, or High).
- [ ] DoD Impact Level alignment verified for any service handling CUI (IL2, IL4, IL5 as applicable).
- [ ] Subprocessor inventory current, with each entry mapped to data types accessed and authorization status.
- [ ] Software supply chain controls documented (signed builds, dependency scanning, software bill of materials where applicable).
- [ ] Hardware supply chain controls documented if hardware procurement is in scope.
- [ ] Annual vendor security review completed for every in-boundary subprocessor.

Section 6: Incident Response and Federal Breach Notification

Federal incident response has stricter notification timelines and content requirements than commercial frameworks. The plan that worked for your Service Organization Control 2 (SOC 2) audit is a starting point, not the finished artifact.

- [ ] Incident response plan written, reviewed in the past 12 months, and aligned to NIST 800-61 guidance.
- [ ] US Computer Emergency Readiness Team (US-CERT) notification process documented, including the one-hour reporting window for federal incidents.
- [ ] Tabletop exercise conducted in the past year with documented results and plan updates.
- [ ] Breach notification procedures cover both regulatory and contractual flowdown notification requirements.
- [ ] Forensic readiness documented (artifact preservation, chain of custody, evidence handling).
- [ ] After-action review process defined, with findings folded back into the POA&M.

Your Path to Authorization: 6-Month Sprint Plan

A clean federal authorization is the output of a working compliance program, not a project. The path below is the 6 months from current state to 3PAO assessment kickoff: the work that has to be done before an assessor can begin a credible review.

The plan assumes a 10-to-100-person SMB starting from a typical pre-authorization posture. Larger teams move slower; SBIR companies with engineering-heavy founding teams sometimes move faster. The cadence is the same.

Month 1: Scope and Path

Goal: Authorization boundary documented and signed off. Target baseline (Low, Moderate, High) selected with rationale. Authorization path chosen. Agency sponsor or JAB pathway initiated.

- **Week 1:** Document the system characterization, data flows, and authorization boundary. Identify every external service the system depends on and the FedRAMP status of each.
- **Week 2:** Complete the FIPS 199 impact categorization. Select your target NIST 800-53 Rev 5 baseline. Document the rationale; this becomes the foundation of your System Security Plan (SSP).
- **Week 3:** Choose the authorization path. Agency ATO is the most common path for SaaS targeting a specific agency; the Joint Authorization Board path covers broader applicability at higher cost and timeline. FedRAMP Tailored LI-SaaS applies only to specific low-impact, low-data-sensitivity systems.
- **Week 4:** Engage your agency sponsor (for agency ATO) or initiate JAB candidacy. Brief the executive sponsor on what the next 5 months will require operationally.

Month 2: SSP and Control Implementation Plan

Goal: First draft SSP circulating. Every control in the selected baseline has a named owner and an implementation summary. Privacy and supply chain control families addressed.

- **Week 5:** Begin SSP drafting using the FedRAMP SSP template. Section 1 through Section 8 are scoping and characterization; most of the work is Sections 9 through 13, which document the controls.
- **Week 6:** Assign every control in the baseline to a named owner. Engineering owns most technical controls; operations owns most administrative; the compliance lead owns governance and oversight.
- **Week 7:** Walk through the Privacy (PT), Supply Chain Risk Management (SR), and Personnel Security (PS) control families. Rev 5 made these more rigorous; many teams gloss over them in the first SSP pass and pay for it during assessment.
- **Week 8:** Complete the first end-to-end SSP draft. Circulate to executive sponsor and any agency sponsor for early-stage feedback. The draft should be substantively complete, not polished; polish happens later.

Month 3: Control Implementation and Evidence Pipeline

Goal: Critical access, logging, and continuous monitoring controls are operating. Evidence is being captured continuously, not under deadline pressure.

- **Week 9:** Stand up the access control posture. MFA on all privileged and remote access, role-based access with documented roles, monthly privileged access review with sign-off, just-in-time emergency access with audit trail.
- **Week 10:** Confirm audit logging covers everything the AU control family requires. Log retention meets your authorization commitment. Implement log heartbeat monitoring so silent log sources fire an alert.
- **Week 11:** Stand up vulnerability scanning at the operating system, web application, and database layers. Monthly cadence. Findings flow directly into the POA&M with named owners and target close dates.
- **Week 12:** Implement the significant change request process. Document the change criteria that trigger Authorizing Official notification. Walk through three recent changes to verify the process produces an audit trail.

Month 4: SSP Polish and Pre-Assessment Readiness

Goal: SSP is assessment-ready. Independent readiness review identifies remaining gaps before 3PAO engagement. Initial POA&M reflects honest current state.

- **Week 13:** Run an internal SSP review with engineering, operations, and the executive sponsor. Hunt for controls described in the SSP that do not match what the system actually does.
- **Week 14:** Engage an independent readiness assessor (typically a different 3PAO, a consultant, or an experienced internal reviewer) to perform a gap analysis. Treat the findings as a free preview of what your 3PAO will find.
- **Week 15:** Close the highest-severity gaps from the readiness review. Move medium-severity items to the initial POA&M with target close dates. Document accepted residual risks.
- **Week 16:** Update the SSP based on remediation work. Lock the SSP version that will be submitted to the 3PAO at kickoff.

Month 5: 3PAO Engagement and Assessment Preparation

Goal: 3PAO under contract. Security Assessment Plan drafted. Evidence package staged. Team practiced enough to maintain the cadence through assessment.

- **Week 17:** Engage two or three 3PAOs for proposals. Compare scope, timeline, pricing, and the lead assessor's experience. Sign with the firm that best matches your size and target authorization path.
- **Week 18:** Develop the Security Assessment Plan (SAP) collaboratively with the 3PAO. The SAP defines scope, methodology, sample sizes, and timeline. It is the document the Authorizing Official will eventually rely on.
- **Week 19:** Stage the assessment evidence package. Folder structure mapped to control families. Files dated within the assessment window. Sample evidence reviewed by the 3PAO so any access or format issues surface before assessment kickoff.
- **Week 20:** Run a final dry-run with engineering and operations. Walk through the controls the 3PAO is most

likely to test first. Confirm everyone knows where their evidence lives.

Month 6: Assessment Kickoff and Submission

Goal: Assessment underway. Security Assessment Report drafting begun. POA&M reflects every finding. Authorization package ready for Authorizing Official review.

- **Week 21:** Assessment kickoff with the 3PAO. Confirm scope, evidence delivery method, sample sizes, and report timeline.
- **Week 22:** Assessor fieldwork. Engineering and operations leads stay available for evidence questions. Findings begin flowing into the draft POA&M.
- **Week 23:** Draft Security Assessment Report (SAR) review. Address material issues that can still be remediated before submission. Document accepted findings for the POA&M.
- **Week 24:** Authorization package submission to the Authorizing Official (for agency ATO) or to the JAB. The package includes SSP, SAR, POA&M, and supporting evidence. Authorization decision typically follows within 60 to 90 days for prepared packages.

By the end of 6 months, your team is positioned to receive an authorization, not just to wait for one. The continuous monitoring discipline that carried you to this point is what will keep the authorization alive through annual assessments and beyond.

Why 6 months and not 12

Twelve to eighteen months is the typical industry timeline for a first FedRAMP authorization from a cold start. Six months is achievable when three conditions are met: the team is fully resourced and not splitting attention with feature work, the cloud environment is already FedRAMP-aligned (cloud provider authorized at your target impact level, services restricted to FedRAMP-authorized offerings), and the agency sponsor or JAB pathway is engaged in parallel with control implementation. SBIR companies and emerging primes who satisfy these three conditions consistently move in months not years. Teams missing any of them should plan for 9 to 12 months. Teams that inherit controls from a pre-authorized shared platform operate against a different timeline because the platform-level controls are already authorized; the team's work narrows to the application layer and assessment focuses on what is unique to the team rather than the underlying infrastructure.

Choosing Your Impact Level: IL2, IL4, or IL5

For SMBs building toward DoD work, the Cloud Computing Security Requirements Guide (CC SRG) Impact Levels matter more than the FedRAMP baselines. The Impact Level determines what data you can handle and which DoD-specific controls apply on top of the FedRAMP baseline.

Impact Level 2 (IL2): Public information and Non-CUI. Applies to information cleared for public release and non-Controlled Unclassified Information (CUI) mission information. The baseline is FedRAMP Moderate plus DoD-specific overlays for personnel security and supply chain risk. Most SBIR Phase I work and many commercial-facing DoD pilots fit IL2.

Impact Level 4 (IL4): Controlled Unclassified Information (CUI). Applies to CUI, including For Official Use Only (FOUO), Privacy Act, and Export Controlled data. The baseline is FedRAMP Moderate plus extensive DoD overlays for boundary protection, encryption, and incident reporting. Most SBIR Phase II and III work touching mission systems sits at IL4.

Impact Level 5 (IL5): CUI with higher sensitivity or mission-critical / NSS data. Applies to information whose unauthorized disclosure could cause serious adverse effects, including mission-critical operational data and certain National Security Systems (NSS) workloads at the unclassified level. The baseline is FedRAMP High plus DoD overlays. Most defense subcontractors supporting fielded systems target IL5.

Impact Level 6 (IL6): Classified information up to Secret. Applies in classified-environment SaaS contexts. Rare at SMB scale; typically reached via partnership with a cleared prime rather than independent authorization.

Picking your target IL

- Default to IL4 if you handle CUI. Most defense subcontractors and Phase II/III SBIR companies do. IL4 is the workhorse impact level for the defense industrial base.
- Step up to IL5 if your data is mission-critical or NSS-adjacent. The IL5 controls are tighter on encryption, boundary protection, and incident reporting; the cost and timeline delta from IL4 is meaningful.
- Step down to IL2 only if you can clearly demonstrate non-CUI status. Many teams default to IL2 to lower cost, then discover during a contract opportunity that their workflow actually touches CUI. Re-categorizing mid-engagement is more expensive than starting at IL4.
- Treat IL6 as a separate conversation. If your roadmap includes classified work, the path runs through cleared facility and personnel posture before it runs through cloud authorization.

Common ATO Findings and How to Avoid Them

These six findings produce more returned ATO packages than any others in our practice. None of them are obscure; all of them are preventable with operational discipline.

1. Identity and Access Management (IAM) debt that nobody owns. Privileged access without documented justification, missing just-in-time access for break-glass operations, missing audit trails for emergency accounts, and stale access that grew with a role and never shrank. This single category produces more six-to-twelve-week

delays than any other in our practice. The fix is monthly privileged access review with named owners and sign-off.

2. An SSP that does not reflect what the system actually does. The SSP should be a current description of how your environment operates, mapped to controls. In practice, SSPs are written for the original assessment and not updated as the system evolves. By re-authorization or the next ConMon review, the SSP and the production environment have diverged enough that the assessor flags the gap. Maintain the SSP the way you maintain your code; it is a system of record, not a deliverable.

3. Audit logs that do not cover the full authorization period. Logs that started capturing midway, that have gaps from silent sources, or that are retained for shorter than the authorization commitment will trigger findings. Implement log heartbeat monitoring and start collection well before assessment kickoff.

4. POA&M that hides instead of tracks. A POA&M missing items the assessor surfaces, or a POA&M with target close dates that never move and never close, signals that the program is not operating continuously. Treat the POA&M as a working backlog with active grooming, not a compliance artifact.

5. Continuous monitoring deliverables that do not arrive monthly. Scan results, POA&M updates, inventory updates, and significant change notifications are the monthly cadence FedRAMP expects. Missing months are not minor; they trigger ConMon escalation and can affect authorization status.

6. Vendor inventory that does not match the actual cloud footprint. A vendor list maintained in a spreadsheet from last year is almost always wrong. Subprocessors with expired authorizations, missing Business Associate Agreements (BAAs) or Data Processing Agreements (DPAs), or undocumented data access get flagged when the assessor cross-references your inventory against the actual data flows.

How to Pick Your 3PAO

The Third-Party Assessment Organization (3PAO) you pick shapes the next 12 months of your authorization program. Most SBIR companies pick the first 3PAO that returns their email; the firms that pick deliberately get cleaner reports, fewer surprises, and lower bills. Eight questions to ask any candidate firm before you sign.

1. How many SBIR-class or SMB-class authorizations have you led in the past 24 months, and at what impact levels?

A 3PAO whose entire book is large-cloud-provider engagements will run your assessment at large-cloud-provider cadence and pricing. A firm with a dozen recent SMB clients at your target impact level will know what assessors look at in your kind of business.

2. What is your pricing structure: fixed fee with milestone billing, or hourly with caps?

Fixed fee with milestone billing is the SMB-friendly default. Hourly with caps can work if the cap is firm. Avoid hourly without a cap.

3. What is your typical timeline from kickoff to Security Assessment Report submission?

Clean assessments at Low or Moderate Impact typically take 8 to 12 weeks of fieldwork plus 3 to 6 weeks for draft and final reports. High Impact runs longer. If a firm cannot describe a baseline timeline, that is a signal.

4. Who will be the lead assessor on my engagement, and can I speak with them before signing?

The lead assessor's experience is the single biggest predictor of assessment quality. Ask for at least 5 years of FedRAMP experience and at least one prior client at your target impact level.

5. What is your remediation philosophy when you find a control gap during fieldwork?

Strong 3PAOs flag gaps early enough that you can remediate before they appear in the SAR. Weak firms document everything as a finding regardless of remediation status.

6. What evidence collection methods do you accept?

Live read-only access to your evidence platform is the lowest-friction path. Confirm the 3PAO accepts what you have.

7. What is your communication cadence during assessment?

Weekly status with named blockers is the SMB-friendly default. Monthly is too sparse; daily is too dense. Confirm there is a named point of contact for the entire assessment window.

8. Can you provide three references at my impact level with current contact information?

A 3PAO that gives you three named clients in your size class and willingly takes a 30-minute call is a 3PAO with strong client relationships.

Red flags

- Pricing is "we will quote after kickoff" with no published structure.
- No SBIR or SMB references; only large-cloud-provider engagements.
- Lead assessor not named, or rotated each engagement.
- No upfront evidence-request list provided.
- More than a 6-week gap between fieldwork and draft SAR.

Green flags

- Published fixed-fee schedule with optional add-ons clearly priced.
- Named lead assessor with 5 or more years of FedRAMP experience and at least one prior client at your impact level.
- Pre-assessment readiness review offered as a separate, smaller engagement.
- Sample evidence-request list provided before contract signing.
- SBIR or SMB-class reference customer willing to take a 30-minute call.

What FedRAMP Authorization Actually Costs

The single most-asked, least-answered question in federal authorization conversations: what does it cost? The numbers below describe the typical SMB range. Your specific cost depends on impact level, environment complexity, authorization path, and whether you build the program internally or rely on shared infrastructure.

3PAO assessment fees

FedRAMP Tailored LI-SaaS assessment	$50,000 to $120,000
FedRAMP Low Impact agency authorization	$80,000 to $180,000
FedRAMP Moderate Impact agency authorization	$150,000 to $350,000
FedRAMP High Impact authorization	$300,000 to $800,000+

Joint Authorization Board (JAB) provisional ATO pathways typically run 20 to 40 percent higher than the equivalent agency authorization for the same impact level due to broader review scope.

Internal time investment

- Compliance lead: 75 to 100 percent of one Full-Time Equivalent (FTE) for the 6-month sprint; 30 to 50 percent steady-state. Often a fractional Chief Information Security Officer (CISO) at SMB scale.
- Engineering team: 400 to 800 hours over the 6-month sprint; 40 to 80 hours per quarter ongoing. Concentrated in Months 2 to 4 of the sprint plan.
- Executive sponsor: 12 to 20 hours per quarter. Reviews program metrics, signs off on risk decisions, attends agency or JAB calls.

Year 1 total budget (all-in)

FedRAMP LI-SaaS at IL2	$150,000 to $400,000
FedRAMP Moderate at IL4 (most common target)	$400,000 to $1,200,000
FedRAMP High at IL5	$1,000,000 to $2,500,000+

These figures are full-burden. They include 3PAO fees, internal labor at fully-loaded rates, cloud infrastructure delta versus a commercial baseline, and continuous monitoring tools.

What pushes the number up

- High Impact baseline selected when Moderate would have served.
- Significant Personally Identifiable Information (PII) in scope, triggering additional privacy controls.
- Complex multi-cloud or hybrid architecture in the authorization boundary.
- Cloud services in use that are not yet FedRAMP authorized at the target impact level, requiring substitution.
- Findings during assessment that require re-testing or extend the authorization window.

Path to lower cost

- Use a pre-authorized shared cloud platform that inherits FedRAMP controls rather than building authorization from scratch. Standalone authorization is the highest-cost path; controlled inheritance from a shared platform is the lowest.
- Start at the lowest defensible impact level. Step up if a contract opportunity requires it.
- Restrict cloud services to FedRAMP-authorized offerings from day one. Substituting services mid-assessment is expensive.
- Run an independent readiness review before engaging a 3PAO for paid assessment. Catching gaps internally is cheaper than catching them under assessment.
- Build internal continuous monitoring discipline. Teams whose ConMon discipline is mature carry that posture

into the assessment and reduce findings.

What an Authorization Evidence Package Looks Like

3PAOs do not want to receive emails with 50 PDFs. They want a single organized package mapped to control families with consistent file naming and timestamps that fall inside the assessment window. The folder structure below is what most SBIR and SMB teams end up with after one authorization cycle; starting with it saves you the cycles.

Folder structure

```
FedRAMP-Authorization-Package-2026/
|-- 00-System-Description/
|   |-- ssp-v3.pdf
|   `-- auth-boundary-diagram.pdf
|-- 01-Governance/
|   |-- compliance-owner-charter.pdf
|   `-- iso-isso-roster.pdf
|-- 02-Access-Control/
|   |-- iam-policy-v2.pdf
|   `-- privileged-access-Q1.xlsx
|-- 03-Audit-Logging/
|   |-- log-retention-policy.pdf
|   `-- log-heartbeat-dashboard.pdf
|-- 04-Change-Management/
|   |-- change-mgmt-policy.pdf
|   `-- significant-change-process.pdf
|-- 05-Vulnerability-Management/
|   |-- vuln-scanning-policy.pdf
|   `-- os-scan-results-Q1/
|-- 06-Supply-Chain/
|   |-- subprocessor-inventory-2026.xlsx
|   `-- sbom-current.json
|-- 07-Incident-Response/
|   |-- ir-plan-v4.pdf
|   `-- tabletop-Q2-results.pdf
|-- 08-Risk-Management/
|   |-- risk-assessment-2026.pdf
|   `-- poam-current.xlsx
`-- 09-Continuous-Monitoring/
    |-- conmon-cadence.pdf
    `-- monthly-deliverables-2026/
```

File naming conventions

- Lowercase-hyphenated names. No spaces or special characters.
- Include version numbers for evolving documents (ssp-v3.pdf).
- Include period markers for time-bounded artifacts (2026-Q1).
- Standardize date format (YYYY-MM-DD or YYYY-Q1 through Q4).
- Consistent extensions: .pdf for policies, .xlsx for exports, .csv for raw data.

What 3PAOs prefer

- Live read-only access to your evidence platform OR a single shared cloud folder.
- Single source of truth; avoid emailing PDFs back and forth.
- Files dated within the assessment window; historical context clearly tagged.
- Documentation of when each artifact was generated and by whom.

Scoring

Total possible: 36 items implemented.

30 to 36 items	Authorization-ready. Engage a 3PAO for assessment kickoff with confidence.
22 to 29 items	Foundations are forming, but address remaining gaps before paid assessment to avoid extending the authorization window or receiving a returned package.
Below 22 items	Significant gaps. Start with authorization boundary, control selection, and continuous monitoring before engaging a 3PAO. An independent readiness review is the most cost-effective next step.

A team scoring 30 or higher will not be common on first pass. That is intentional. The bar is calibrated to identify the teams ready to start a credible assessment, not to clear every team that has read the framework.

Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 36 items with the team and mark each one. The page is designed to live on a wall or in a binder for the duration of your prep.

1. Authorization Scope and System Boundary

- ☐ Authorization boundary diagram drafted _____
- ☐ System characterization documented _____
- ☐ FIPS 199 impact categorization completed _____
- ☐ External services and interconnections inventoried _____
- ☐ Data flow diagram for CUI or sensitive data _____
- ☐ Authorization path selected _____

2. NIST 800-53 Rev 5 Control Selection

- ☐ Target baseline selected with rationale _____
- ☐ Control implementation summary drafted _____
- ☐ Tailoring decisions documented _____
- ☐ Compensating controls documented _____
- ☐ Privacy controls (PT family) addressed _____
- ☐ Supply Chain Risk Management (SR) implemented _____

3. Continuous Monitoring and POA&M

- ☐ OS, web app, and database vulnerability scanning monthly _____
- ☐ POA&M tracking active with owners and dates _____
- ☐ Significant change request process documented _____
- ☐ Annual security assessment scoped with 3PAO _____
- ☐ Monthly ConMon deliverables process defined _____
- ☐ Continuous monitoring metrics reviewed quarterly _____

4. Identity, Access, and Audit Logging

- ☐ MFA enforced (FIPS 140-validated) _____
- ☐ Role-based access aligned to least privilege _____
- ☐ Privileged access reviewed monthly _____
- ☐ Just-in-time emergency access _____
- ☐ Audit logging covers NIST AU control content _____
- ☐ Log retention meets authorization commitment _____

5. Supply Chain and FedRAMP-Authorized Services

- ☐ Cloud services verified FedRAMP authorized _____
- ☐ DoD Impact Level alignment verified _____
- ☐ Subprocessor inventory current with data mapping _____
- ☐ Software supply chain controls documented _____
- ☐ Hardware supply chain controls documented (if in scope) _____
- ☐ Annual vendor security review completed _____

6. Incident Response and Federal Breach Notification

- [ ] IR plan reviewed in past 12 months _____
- [ ] US-CERT notification process documented _____
- [ ] Tabletop exercise documented in past year _____
- [ ] Breach notification covers regulatory and contractual _____
- [ ] Forensic readiness documented _____
- [ ] After-action review feeds back to POA&M _____

Total implemented (out of 36): _____

30 to 36: Authorization-ready. Engage 3PAO.
22 to 29: Foundations forming; close gaps before paid assessment.
Below 22: Significant gaps; start with boundary, control selection, and ConMon.

A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business (WOSB) and an Amazon Web Services (AWS) Advanced Tier Partner with a Defense Counterintelligence and Security Agency (DCSA) Secret-level Facility Clearance and Cybersecurity Maturity Model Certification (CMMC) Level 2 self-assessment status. Our founding team holds active Secret and higher clearances. We help SBIR companies, defense subcontractors, and emerging primes build authorized cloud environments and operate them through every assessment window.

Our Bridge platform delivers ATO inheritance at IL2, IL4, and IL5, FedRAMP-aligned continuous monitoring, and CSSP integration on a subscription model. For teams pursuing federal authorization for the first time, inheriting controls from a shared platform is materially cheaper and faster than building authorization from scratch.

If you are using this checklist to assess your own readiness and want a second set of eyes on your scoring, or if you are pursuing FedRAMP alongside CMMC or DoD impact-level alignment, we are happy to help.

For the architectural starting point that pre-satisfies most of this checklist by design, the Cloud Landing Zones Guide is our 28-page tactical playbook for compliance-first multi-account architecture. A landing zone built per the Guide inherits approximately 40 percent of FedRAMP Moderate controls from AWS, leaving a cleaner scope of customer-implemented controls to address. Free at pandoracloud.net/cloud-landing-zones-guide.

Run the numbers for Impact Level 2, 4, and 5 in two clicks: pandoracloud.net/cost-calculator/. The Calculator includes FedRAMP and NIST 800-53 Revision 5 control inheritance in the math.

Ready for a second set of eyes on your readiness?

Schedule a free 30-minute consultation. We will walk through your scored checklist and help you prioritize the next 6 months.

pandoracloud.net/#schedule-consultation

Glossary

For readers new to FedRAMP and NIST 800-53 vocabulary, this glossary names the most common terms referenced in this checklist.

3PAO (Third-Party Assessment Organization)
A FedRAMP-accredited assessor authorized to evaluate cloud services for federal authorization. The 3PAO produces the Security Assessment Report (SAR) the Authorizing Official relies on.

Authorization Boundary
The set of components, data flows, and personnel within the scope of an authorization. Drawing the boundary correctly is the single most consequential scoping decision in an authorization.

Authorizing Official (AO)
The senior federal official with authority to accept the risk of operating a system. In agency ATO paths, the AO is at the sponsoring agency; in JAB paths, the AO authority sits with the Joint Authorization Board.

cATO (Continuous Authorization to Operate)
An authorization model in which the system maintains an active authorization through continuous monitoring rather than calendar-based re-authorization. Replacing the traditional one-to-three-year ATO model in many DoD program offices.

CC SRG (Cloud Computing Security Requirements Guide)
The DoD-specific guidance that adds Impact Level requirements on top of the FedRAMP baseline for cloud services handling DoD data.

ConMon (Continuous Monitoring)
The ongoing operational discipline of monthly scans, POA&M updates, and significant change notifications that maintains an authorization in good standing.

FedRAMP (Federal Risk and Authorization Management Program)
The federal government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services.

FedRAMP Tailored / LI-SaaS
A FedRAMP authorization path designed for low-impact Software-as-a-Service offerings, with a reduced control set.

Impact Level (IL)
The DoD CC SRG categorization of data sensitivity. IL2 covers public and non-CUI; IL4 covers CUI; IL5 covers CUI with higher sensitivity or National Security Systems data; IL6 covers Secret-classified information.

Joint Authorization Board (JAB)
The board of Chief Information Officers from DoD, the Department of Homeland Security (DHS), and the General Services Administration (GSA) that issues provisional ATOs (P-ATOs) for cloud services with broad federal applicability.

NIST 800-53 Rev 5
The current revision of the NIST control catalog. Published September 2020, it superseded Rev 4 and introduced privacy controls and Supply Chain Risk Management as integrated families.

NIST 800-171

The 110-requirement standard for protecting Controlled Unclassified Information (CUI) in non-federal systems. The basis for the CMMC Level 2 assessment.

POA&M (Plan of Action and Milestones)

The structured tracking of open findings with owners and target close dates. Required as part of every FedRAMP authorization and updated monthly during ConMon.

SAP (Security Assessment Plan)

The 3PAO-authored plan that defines assessment scope, methodology, sample sizes, and timeline. Approved before assessment kickoff.

SAR (Security Assessment Report)

The 3PAO-authored report documenting assessment findings. Submitted to the Authorizing Official as part of the authorization package.

SSP (System Security Plan)

The vendor-authored description of how the system operates, how each control in the selected baseline is implemented, and how the operational posture maintains the controls over time. The largest single artifact in an authorization package.