PANDORA CLOUD
UNPACKING COMPLEXITY

# ATO Readiness Checklist

28 controls every SMB pursuing federal authorization should have in place. Plus a 90/60/30-day pre-authorization path.

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

If your business is pursuing an Authority to Operate (ATO) for a federal agency, a Federal Risk and Authorization Management Program (FedRAMP) authorization for a cloud service, a Department of Defense (DoD) Cloud Service Provider Security Requirements Guide (CSP SRG) Impact Level (IL) authorization, or Cybersecurity Maturity Model Certification (CMMC) Level 2 certification, this checklist tells you in fifteen minutes whether your operation is ready for assessment, where the gaps are, and what the next 90 days should look like.

It is for SMB owners, compliance leads, security leads, and program managers preparing for any of those authorizations for the first time. The 28 items below cover the five areas where SMBs most frequently stall before authorization, mapped to specific National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 control families and the artifacts assessors actually ask for.

The most useful insight in this checklist is not the score. It is the 90/60/30-day pre-authorization timeline that follows it. Most ATO efforts fail not because the controls are not implemented but because the package is not assembled and presented on the back-loaded timeline that authorization decisions actually run on.

# Why ATO Readiness Matters Now

The federal authorization landscape has moved meaningfully over the past two years.

**FedRAMP Revision 5 transition completed in 2024-2025.** Cloud Service Providers (CSPs) holding Provisional Authority to Operate (P-ATO) status from the Joint Authorization Board (JAB) or agency authorizations from individual federal sponsors completed transition to NIST 800-53 Revision 5 control baselines. New authorization packages submitted today are evaluated against Revision 5; older Revision 4 packages are no longer accepted.

**CMMC 2.0 Phase 1 began November 10, 2025.** DoD contractors handling Federal Contract Information (FCI) must self-attest to CMMC Level 1 today, and contractors handling Controlled Unclassified Information (CUI) must self-assess to Level 2 and affirm annually under Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7021. Phase 2 (Level 2 third-party assessments via CMMC Third-Party Assessment Organizations, or C3PAOs) was scheduled for November 10, 2026; DoD suspended it on July 13, 2026 pending a CMMC Reform Task Force review, and no new date has been announced. If you sell to defense agencies under CUI contracts, plan for third-party assessment on a date not yet set.

**Agency ATO timelines have not gotten shorter.** Risk Management Framework (RMF) authorization through agency Authorizing Officials (AOs) still typically runs 6 to 18 months from kickoff to ATO letter, depending on system criticality, agency rigor, and how prepared the System Owner walks in. The single biggest lever on that timeline is how complete the Body of Evidence is when assessment begins.

**Continuous Authorization to Operate (cATO) is the direction of travel.** The DoD's cATO model (and similar agency efforts) replaces the three-year point-in-time ATO renewal with continuous monitoring evidence streams. Organizations preparing for ATO today should be thinking about how to instrument the controls so that ongoing

evidence collection is automatic, not a fire drill at three-year reauthorization.

The 28-item checklist below is the floor. The 90/60/30-day pre-authorization timeline is the path. The authorization-route selection section helps you pick which destination to head toward.

## What ATO Actually Requires

Before scoring yourself, a quick orientation on the federal authorization landscape. There is no single "ATO process"; there are several authorization paths, each with different sponsors, baselines, and assessor types.

**Agency Authorization to Operate (ATO) via the Risk Management Framework (RMF).** Defined in NIST SP 800-37 Revision 2. Six steps: Categorize, Select, Implement, Assess, Authorize, Monitor. The system owner builds the package; an agency Assessment and Authorization (A&A) team or contracted independent assessor performs the assessment; the agency Authorizing Official (AO) signs the ATO letter. Used by every federal agency for systems they operate or sponsor. NIST SP 800-53 Revision 5 controls form the baseline.

**Federal Risk and Authorization Management Program (FedRAMP).** Standardizes authorization for cloud services used by federal agencies. Three baselines (Low, Moderate, High) mapped to NIST 800-53 Revision 5 control selections. Two paths: agency-sponsored ATO (one agency authorizes, others reuse via package readability) or Joint Authorization Board P-ATO (the JAB authorizes, every federal agency may reuse). Third Party Assessment Organizations (3PAOs) perform the security assessment.

**DoD Cloud Service Provider Security Requirements Guide (CSP SRG) Impact Levels.** IL2 (public/non-CUI), IL4 (CUI, and most defense contract work), IL5 (unclassified National Security Systems; CUI only where an Authorizing Official requires it), IL6 (Secret-level classified). Cloud services serving DoD must be authorized at the appropriate Impact Level. IL2 typically requires FedRAMP Moderate as a baseline; IL4 and IL5 require FedRAMP High plus DoD-specific overlays.

**CMMC 2.0.** DoD's certification model for contractors handling FCI or CUI. Three levels: Level 1 (FCI, self-assessment), Level 2 (CUI, third-party C3PAO assessment for most contracts), Level 3 (advanced persistent threat protection, government-led assessment). Maps to NIST 800-171 Revision 2 control families (CMMC has not yet adopted Revision 3).

**The overlap is significant.** All four paths share the same NIST 800-53 / 800-171 control vocabulary. A control well-implemented for one path typically satisfies most of the others, with framework-specific overlays. This is why the cross-framework approach saves so much work for SMBs pursuing multiple authorizations.

## How to Use This Checklist

Walk through the 28 items below with your team. For each item, mark one of:

- Implemented: the control is in place and you have evidence (artifact, screenshot, or auditor-ready document).
- Partial: the control is partially in place; gaps exist or evidence is incomplete.
- Missing: the control does not exist or has not been documented.

Count the implemented items. Use the scoring tiers to determine your readiness state. Then read the 90/60/30-day timeline to map the next quarter of work.

## Section 1: Governance and Ownership

Authorization packages need a single point of accountability. Most SMB ATO failures begin here: ownership ambiguity, missing executive sponsorship, or a compliance lead who is also the systems administrator and runs out of bandwidth in the assessor's third week.

- [ ] Compliance owner identified with explicit authority to sign packages and represent the organization to assessors and the AO.
- [ ] Security lead assigned with technical authority over security architecture decisions.
- [ ] Technical lead assigned with operational authority over infrastructure and configuration baselines.
- [ ] Authorization path identified (agency ATO, FedRAMP, IL2/IL4/IL5, or CMMC Level 1/2/3).
- [ ] Budget allocated for authorization activities including assessor fees, control implementation, and continuous monitoring tooling.
- [ ] Executive sponsor engaged at the level of an officer or partner; ATO escalations have an unblocking path.

## Section 2: Scope and Boundaries

The single most common 3PAO finding on first-time authorization packages is unclear authorization boundary. Spending time on the boundary diagram up front prevents late-stage scope changes that re-trigger assessment work.

- [ ] Authorization boundary defined in writing and validated against the system architecture.
- [ ] In-scope systems, data flows, and external integrations documented.
- [ ] Shared responsibility model mapped (cloud provider responsibilities vs. customer responsibilities for every control).
- [ ] Third-party services and Software-as-a-Service (SaaS) integrations inventoried with FedRAMP authorization status verified for each.
- [ ] Data classification completed (Federal Information Processing Standards (FIPS) 199 categorization for confidentiality, integrity, availability).
- [ ] Network diagrams current, accurate, and signed off by the technical lead.

## Section 3: Documentation Body

Documentation is where ATO packages fail visibly. Assessors expect specific artifacts in specific formats; missing or stale documents are immediate evidence of program immaturity.

- [ ] System Security Plan (SSP) written using NIST SP 800-18 guidance, current within the last 12 months, all required sections complete.
- [ ] Security policies covering all required NIST 800-53 control families (or 800-171 for CMMC), reviewed within the last 12 months.
- [ ] Standard Operating Procedures (SOPs) documented for key operational activities (account management, change control, incident response, configuration management).
- [ ] Incident Response Plan (IRP) documented per NIST SP 800-61 and tested with at least one tabletop exercise within the last 12 months.
- [ ] Configuration Management Plan documented; baseline configurations defined for in-scope systems.
- [ ] Contingency Plan / Information System Contingency Plan (ISCP) per NIST SP 800-34, with backup, recovery, and disaster recovery procedures and a test record.

## Section 4: Technical Controls

Technical controls are the substance of the authorization. Six controls below close the gaps most-often called out in 3PAO Security Assessment Reports (SARs).

- [ ] Multi-factor authentication enforced for all users with privileged access to in-scope systems (Identification and Authentication (IA) family).
- [ ] Role-based access control with least-privilege permissions for every workforce member; access reviews documented quarterly (Access Control (AC) family).
- [ ] Encryption at rest using FIPS 140-3 validated cryptographic modules for all in-scope storage; encryption in transit using TLS 1.2 or higher (System and Communications Protection (SC) family).
- [ ] Audit logging enabled across all in-scope systems with retention meeting agency or framework requirements (typically 1 year online, 3 years archive minimum); log integrity protected (Audit and Accountability (AU) family).
- [ ] Vulnerability scanning running at a defined cadence (typically monthly minimum, weekly recommended for FedRAMP Moderate+); critical and high findings remediated within Service Level Agreement (SLA) windows defined in the SSP (Risk Assessment (RA) family).
- [ ] Configuration management enforced via baselines, change control records, and automated drift detection (Configuration Management (CM) family).

## Section 5: Evidence Collection and Remediation

Authorization decisions are made on evidence, not claims. The Body of Evidence (BoE) is the package the AO actually reviews; gaps here turn into either ATO denial or ATO with significant Plan of Action and Milestones (POA&M) conditions.

- [ ] Evidence collection process defined (manual artifact gathering, automated control testing, or hybrid) with clear ownership for each control.

- [ ] Evidence mapped to specific control requirements; each control has an artifact pointer (file path, ticket reference, or system query).
- [ ] Plan of Action and Milestones (POA&M) maintained tracking known gaps, owners, target completion dates, and remediation status.
- [ ] Known gaps prioritized by risk and assigned to named owners with realistic target dates (not "Q3 2026" with no specifics).
- [ ] Remediation progress reviewed at minimum monthly; POA&M aging tracked.
- [ ] Previous assessment findings (from internal audits, prior 3PAO assessments, or red-team exercises) addressed and documented as closed or accepted.

# Cross-Authorization Path Overlap: Implement Once, Authorize Many

Most SMBs pursuing federal authorization implement controls separately for each path, write nearly identical policies for each, and burn engineering cycles maintaining redundant evidence packages. The better approach is to map controls cross-path first, then produce path-specific evidence views from the same underlying work.

| Control area | NIST 800-53 R5 | FedRAMP overlay | DoD CC SRG | 800-171 (CMMC |
|---|---|---|---|---|
| Multi-factor authentication | IA-2 | IA-2 (1)(2)(11)(12) | + DoD MFA tokens IL5 | 3.5.3 |
| Encryption at rest | SC-28 | SC-28 (1) FIPS 140-3 | Same | 3.13.11 |
| Encryption in transit | SC-8 | SC-8 (1) FIPS 140-3 | Same | 3.13.8 |
| Audit logging | AU-2, AU-3 | + SIEM integration | + DoD log agg IL4+ | 3.3.1, 3.3.2 |
| Continuous monitoring | CA-7 | + FedRAMP ConMon SLAs | + DoD ConMon | 3.12.3 |
| Vulnerability scanning | RA-5 | Monthly cadence | + DoD scan tools | 3.11.2 |
| Incident response | IR-4 | + US-CERT reporting | + DoD CERT reporting | 3.6.1, 3.6.2 |
| Configuration management | CM-2, CM-3 | Same | Same | 3.4.1, 3.4.2 |
| Risk assessment | RA-3 | Same | Same | 3.11.1 |
| System security plan | PL-2 | FedRAMP template | DoD template | 3.12.4 |

Every authorization path uses NIST 800-53 (or 800-171 for CMMC) as the underlying control vocabulary. Implement once at the highest baseline you expect to need; document the implementation; produce path-specific evidence packages from the same controls.

# Scoring

Total items implemented (out of 28):

- 🟢 **23 to 28 items** — Strong posture. Ready to engage an assessor or 3PAO. Focus next on continuous monitoring instrumentation so the next reauthorization is evidence-driven, not a rebuild.
- 🟡 **15 to 22 items** — Foundations forming, gaps remain. Address the gaps via the 90/60/30-day timeline below before scheduling assessment. Engaging an assessor with foundational gaps wastes assessor time and your money.
- 🔴 **Below 15 items** — Significant gaps. Authorization is at material risk. Start with Section 1 (Governance) and Section 3 (Documentation); without those, no amount of technical implementation will pass.

# What to Do With Your Score

The score is only useful if it points to a specific next move.

**If you scored 23-28 (Strong):** Your foundation is in place. The next investment is either engaging the assessor (3PAO for FedRAMP, CAP/IAP for agency ATO, C3PAO for CMMC Level 2) or instrumenting continuous monitoring so your reauthorization three years from now is a drift check rather than a rebuild. If you have not yet selected an assessor, the assessor selection criteria below are your starting point.

**If you scored 15-22 (Foundations Forming):** The gaps you have are likely concentrated in Documentation (Section 3) or Evidence Collection (Section 5). The 90/60/30-day timeline below targets exactly those gaps. Pick the section where you have the lowest score and work through it first.

**If you scored below 15 (Significant Gaps):** You are carrying material risk on authorization. Most SMBs in this state stall not at assessment but at the ATO decision: the package gets returned because Body of Evidence cannot be assembled. Start with Days 1-30 of the timeline; the early items (governance, scope, SSP) are the ones that unblock everything else.

# Your 90/60/30-Day Pre-Authorization Timeline

This timeline targets teams scoring Yellow or Red on the 28-item checklist. Strong-foundation teams can compress it; teams with significant gaps may need 120 days.

The timeline runs backwards from your assessment date. Day 1 of the timeline is 90 days before assessor kickoff; Day 90 is the day the assessor walks in. Most SMBs build forward from "today" and miss that the back end of the timeline (the 30-day pre-assessment window) is the most evidence-intensive.

## Days 1 to 30 (T-90 to T-60): Foundation and scope

**Goal:** Authorization boundary defined, ownership assigned, SSP draft written, FIPS 199 categorization complete.

- **Day 1-3:** Identify compliance owner, security lead, technical lead. Document executive sponsor and escalation path. Confirm authorization path (agency ATO, FedRAMP, IL2/IL4/IL5, CMMC Level).
- **Day 4-7:** Define authorization boundary. Inventory in-scope systems, data flows, and external integrations. Validate against architecture diagrams.
- **Day 8-14:** Complete FIPS 199 categorization. Determine baseline (Low / Moderate / High for FedRAMP; CMMC Level 1/2/3 for DoD contractors). Confirm overlay requirements (DoD IL2/IL4/IL5 if applicable).
- **Day 15-21:** Draft SSP using NIST SP 800-18 guidance. Use the FedRAMP SSP template if pursuing FedRAMP, or your agency's SSP template for agency ATO.
- **Day 22-28:** Map shared responsibility (cloud provider vs. customer responsibilities for every control) into the SSP. Verify FedRAMP authorization status of every third-party SaaS in scope.
- **Day 29-30:** Internal SSP review with security and technical leads. Identify any control families with no implementation; flag as Day 31-60 priorities.

## Days 31 to 60 (T-60 to T-30): Implementation and evidence assembly

**Goal:** All in-scope controls implemented; evidence collected and mapped; POA&M established for residual gaps.

- **Day 31-37:** Close any control gaps identified in Day 29-30 review. Most common: MFA enforcement on a missed system, encryption-at-rest on a backup store, audit logging on a forgotten service.
- **Day 38-44:** Implement evidence collection process. For each in-scope control, document the artifact source (config file, ticket reference, system query). Build the artifact catalog.
- **Day 45-51:** Run a full internal control assessment using the NIST 800-53A or 800-171A assessment procedures. This is the rehearsal for the formal assessment. Document findings.
- **Day 52-58:** Establish POA&M. Every gap from Day 45-51 gets an owner, target date, and risk rating. POA&M aging tracking begins.
- **Day 59-60:** Update SSP to reflect final implementation state. Lock SSP version. Begin assembling the Body of Evidence package.

### Days 61 to 90 (T-30 to assessment): Package finalization and assessor preparation

**Goal:** Body of Evidence complete, SSP final, assessor selected and onboarded, internal team rehearsed.

**Day 61-65:** Final SSP review and AO pre-brief. Walk the package through the AO (or designated representative) before the assessor sees it. AO concerns surface here, not in the formal review.

**Day 66-72:** Body of Evidence finalization. Every control has an artifact. Every artifact is current. Cross-reference catalog complete.

**Day 73-79:** Assessor selection if not already complete. For FedRAMP, select a 3PAO from the FedRAMP Marketplace. For agency ATO, work with your sponsoring agency's A&A team. For CMMC Level 2, select a C3PAO.

**Day 80-86:** Assessor kickoff prep. Brief the team on what to expect, who answers what, and how interview-style assessment questions are typically asked. Schedule key technical interviews.

**Day 87-89:** Final dry run. Walk one control end-to-end as if the assessor is in the room. Catch any missing artifacts now, not during fieldwork.

**Day 90:** Assessor kickoff. Body of Evidence delivered. SSP delivered. Schedule confirmed.

## Common Patterns We See

Across SMBs pursuing federal authorization, the same five gaps show up over and over.

**1. The "we'll figure out the boundary later" gap.** Authorization boundary is the first thing the AO reviews and the last thing the SMB defines. Defining it on Day 1 saves 30+ days of rework when the assessor finds in-scope systems missing from the SSP.

**2. The "documentation is just paperwork" mindset.** Documentation is the assessor's primary evidence source. A current, accurate SSP with mapped controls and artifact pointers is the difference between an ATO and an "ATO with conditions" (a hedge that often blocks contract award).

**3. The control inheritance over-claim.** SMBs running on a FedRAMP-authorized cloud assume too much control inheritance. The cloud provider's authorization covers the platform; you still own configuration, access, and audit logging. SMBs that claim full inheritance get those claims rejected at SAR review.

**4. The continuous monitoring afterthought.** ConMon requirements are non-negotiable post-ATO and frequently weak in the package itself. Build ConMon evidence streams during pre-authorization, not after; the assessors will check and the AO will issue conditional ATOs if they are not present.

**5. The single-author SSP problem.** Senior SSPs that look professional are written by someone who has been through ATO before; SMBs writing their first SSP without that authority almost always need a rewrite cycle. Hiring a federal compliance consultant for a 40-hour SSP review pass typically saves 80+ hours of rewrite cycles.

If you scored Yellow or Red, at least three of these patterns are almost certainly the cause.

# Authorization Path Selection

If you have not yet locked in your authorization path, this section helps you pick.

**Agency ATO via Risk Management Framework.** Pick this if you operate a system on behalf of a single federal agency, your contract requires authorization for that agency only, and the agency has its own A&A team. Timeline: typically 6 to 18 months. Cost: implementation costs vary widely; assessor cost is bundled into the contract. Reuse: limited; each agency typically requires its own ATO process.

**FedRAMP agency-sponsored ATO.** Pick this if you offer a cloud service intended for use by multiple federal agencies and you have a sponsoring agency willing to authorize first. Timeline: typically 12 to 24 months. Cost: $250,000 to $1,000,000+ for full FedRAMP Moderate (3PAO assessment + ConMon tooling + dedicated compliance staff). Reuse: high; once authorized, every other agency may reuse the package.

**FedRAMP JAB P-ATO.** Pick this if you are a high-volume cloud service provider with strategic federal market positioning and the resources to navigate a multi-year, JAB-prioritized process. Timeline: typically 18 to 36 months. Cost: similar to agency-sponsored but with tighter timelines and higher rigor. Reuse: highest; JAB authorization is the gold standard.

**DoD CC SRG IL4/IL5 authorization.** Pick this if you serve DoD with CUI workloads. Requires FedRAMP Moderate (IL4) or High (IL5) as a baseline plus DoD-specific overlays. Timeline: 18 to 36 months from FedRAMP completion to IL5 authorization. Cost: substantial; IL5 typically adds 30-50% on top of FedRAMP High costs.

**CMMC Level 2 certification.** Pick this if you sell to DoD and your contracts handle CUI. Level 2 self-assessment under DFARS 252.204-7021 applies today; the Phase 2 shift to C3PAO assessment for most DoD CUI contracts was suspended by DoD on July 13, 2026 and will return on a date not yet announced. Timeline: 6 to 12 months from gap analysis to C3PAO assessment. Cost: typically $50,000 to $250,000 for SMB scope (C3PAO assessment + remediation + ongoing ConMon).

The right path for most SMBs: start with the smallest authorization that satisfies your nearest contract requirement, then expand. CMMC Level 2 is often the entry point for defense contractors; agency ATO is often the entry point for civilian-agency systems; FedRAMP is the entry point for cloud service providers.

# Cost Expectations

What does pre-authorization actually cost an SMB? Honest ranges, with what pushes them up and how to hold them down.

**CMMC Level 2 (most-asked).** $50,000 to $150,000 for typical SMB scope: gap analysis ($10-25k), remediation ($20-75k), C3PAO assessment ($15-50k), ongoing continuous monitoring tooling ($10-25k/year). Pushed up by complex network architectures, multi-cloud environments, and shadow IT discovery during assessment. Held down by clear scope, automation-first control implementations, and starting with a 90-day gap analysis before committing to assessment.

**Agency ATO via RMF.** $50,000 to $500,000 implementation cost; assessor cost is typically bundled into the contract (the agency's A&A team is funded by the agency). Pushed up by complex authorization boundaries, control inheritance disputes, and SSP rewrite cycles. Held down by hiring a federal compliance consultant for a 40-hour SSP review before assessor kickoff.

**FedRAMP Moderate (agency-sponsored).** $250,000 to $1,000,000+. 3PAO assessment alone runs $150,000 to $500,000 depending on scope. ConMon tooling, dedicated compliance staff, and security architecture investments add the rest. Pushed up by missing baselines (forces architecture changes mid-flight), SaaS dependencies that are not FedRAMP-authorized, and inadequate continuous monitoring instrumentation. Held down by selecting a strong sponsoring agency, locking baseline early, and building automated evidence pipelines from Day 1.

**FedRAMP High / DoD IL5.** $750,000 to $3,000,000+. The tail end of cost ranges; only worth pursuing for cloud service providers with strategic federal market positioning.

**The cheapest move:** Start with the smallest authorization that unlocks your contract pipeline. A $75k CMMC Level 2 certification often delivers more contract value per dollar than a $1M FedRAMP Moderate for an SMB with a defense-only customer base.

## Assessor Selection Criteria

For FedRAMP and CMMC Level 2, you select your own assessor. Selection criteria matter; an experienced 3PAO or C3PAO accelerates the timeline, while an inexperienced assessor often extends it.

- Experience with your authorization path. A 3PAO that has done 50 FedRAMP Moderate assessments is faster than one that has done 5. A C3PAO with CMMC Level 2 assessments under their belt is faster than one whose first assessments are with you.
- Experience with your technology stack. A 3PAO that knows AWS GovCloud reads your evidence faster than one that learned it on your engagement. The same applies to Azure Government, Google Cloud for Government, and on-premises private cloud.
- Industry experience. A 3PAO that has assessed similar SMB engagements understands the constraints; one whose primary clients are large enterprises often applies enterprise-scale expectations to an SMB-scale package.
- Communication style. ATO assessments are intensely communicative; you will spend dozens of hours on technical interviews. An assessor who explains findings clearly and works collaboratively saves weeks compared to one who issues findings without context.
- Reference checks. Ask for two reference clients of similar scope. Talk to the compliance owner at each. The most consistent feedback signal is whether the engagement timeline matched the proposal.
- Capacity. A 3PAO that can start within 30 days of contract is materially better than one that books 6 months out. ATO timelines are unforgiving of assessor scheduling delays.

The lowest-cost 3PAO is rarely the cheapest path to ATO. Cost-per-month-of-elapsed-time matters more than cost-per-assessor-day.

# A Worked Example

A 22-person defense-tech SMB pursuing CMMC Level 2 certification scored 11 of 28 on this checklist. The CEO believed they were "compliant" because they used Microsoft 365 GCC High and AWS GovCloud, had drafted policies the year before, and had not had a security incident.

The 17 missing items included: SSP older than 18 months and not aligned to NIST 800-171 control families, no formal authorization boundary diagram, no evidence collection process, MFA enforced on email but not on AWS console access, no IR plan tested in the last 12 months, no continuous monitoring instrumentation, no POA&M for known gaps, and no formal C3PAO selected.

They worked the 90-day timeline. By Day 30 they had: rewritten the SSP to current state, defined the boundary, documented shared responsibility with both Microsoft and AWS, completed FIPS 199 categorization. By Day 60 they had: closed 6 control gaps identified in internal assessment, established the POA&M, instrumented basic continuous monitoring via AWS Config and Microsoft Purview. By Day 90 they had: completed AO pre-brief, finalized Body of Evidence, selected and onboarded a C3PAO, completed dry-run.

They scored 25 of 28 on the re-take; the remaining gaps were continuous monitoring depth (deferred to first ConMon cycle) and formal red-team exercise (deferred to Year 2 of CMMC Level 2 maintenance).

The cost: roughly 240 hours of compliance owner time, 180 hours of contracted federal compliance consultant time, $32,000 in C3PAO assessment fees, and $18,000 in continuous monitoring tooling. Total: roughly $115,000 over the 90 days plus $15,000 in ongoing annual ConMon costs.

The result: they passed C3PAO assessment and received CMMC Level 2 certification on schedule, then signed a $2.4M three-year prime contract that had been gated on certification. The 28-item checklist was the diagnostic. The 90/60/30-day timeline was the prescription. The contract was the outcome.

# Where to Go From Here

The ATO Readiness Checklist sits in a longer compliance journey. Depending on your authorization target and your buyers, the natural next moves:

**If you scored Yellow or Red:** Start with the 90/60/30-day timeline. Re-score at Day 30 to measure progress.

**If your landing zone is informal or undocumented:** Pick up the Cloud Landing Zones Guide. The architectural foundation pre-satisfies most of the NIST 800-53 Rev 5 controls this checklist references; the faster your authorization timeline, the more leverage a deliberate landing zone produces. Free at pandoracloud.net/cloud-landing-zones-guide.

**If you are pursuing FedRAMP Moderate or High specifically:** Pick up the FedRAMP/NIST Readiness Checklist when it ships in September. Free at pandoracloud.net/fedramp-nist-checklist.

**If you also handle PHI or cardholder data:** Pick up the HIPAA/PCI Readiness Checklist. Many ATO controls satisfy HIPAA and PCI DSS simultaneously. Free at pandoracloud.net/hipaa-pci-checklist.

**If enterprise commercial buyers are also asking for SOC 2 Type II:** Pick up the SOC 2 Readiness Checklist. The controls you have already implemented for ATO satisfy most of SOC 2's Security trust services criterion. Free at pandoracloud.net/soc2-readiness-checklist.

**If you have not yet established the cloud foundation:** Take the Cloud Compliance Foundation Worksheet first. It is the entry-point assessment that this checklist builds on. Free at pandoracloud.net/foundation-worksheet.

**If you want the cross-framework view across all paths:** Pick up the Future of Cloud Compliance Whitepaper. It includes a 25-row cross-framework control mapping. Free at pandoracloud.net/future-of-compliance-whitepaper.

In every case, NIST 800-53 Revision 5 or NIST 800-171 (for CMMC) is the underlying control vocabulary. Implement once at the highest baseline you expect to need; produce path-specific evidence packages from the same controls.

## Framework Updates to Watch

The compliance landscape is in motion. The citations and controls in this checklist are accurate as of May 2026, but several frameworks have updates in progress that will affect how organizations document and demonstrate authorization readiness over the next 12 to 24 months. If your readiness work is anchored to current rule citations, you are correctly positioned for today; this section names what to watch for.

**NIST 800-53 Rev 5 (stable).** Released in 2020; point releases 5.1.1 (November 2023) and 5.2.0 (August 2025). NIST has indicated Rev 6 work is in early discussion but no public draft is available; a Rev 6 release is several years out. New ATO and FedRAMP packages today are evaluated against Rev 5.

**FedRAMP (aligned with NIST 800-53 Rev 5).** FedRAMP officially moved to Rev 5 in May 2023 with phased Cloud Service Provider transition through 2024 and 2025. All new packages submitted today are Rev 5. The FedRAMP Program Management Office continues to evolve continuous monitoring expectations and authorization-package automation; check the FedRAMP Marketplace for current 3PAO availability and authorization-status changes.

**CMMC 2.0 (Phase 1 in force; Phase 2 suspended).** The DoD final rule became effective December 16, 2024 with a four-phase rollout: Phase 1 (Level 1 / Level 2 self-assessments) started November 10, 2025 and remains in force; Phase 2 (Level 2 third-party assessments via C3PAOs) was scheduled for November 10, 2026, with Phase 3 (Level 3) and Phase 4 (full implementation) to follow in 2027 and 2028. On July 13, 2026 DoD suspended Phase 2 and the later milestones until further notice, pending a 60-day CMMC Reform Task Force review with a report due in mid-September 2026. Phase 1 obligations under DFARS 252.204-7021 (self-assessment and annual affirmation) are unaffected. If your business sells to defense agencies, the return of third-party assessment is the change most likely to affect contract eligibility, on a date not yet announced.

**NIST 800-171 Rev 3 (published, not yet adopted by CMMC).** NIST published 800-171 Rev 3 in May 2024. CMMC Level 2 currently still references Rev 2; the DoD timeline for Rev 3 adoption is unclear but expected in 2026 or 2027. Industry refers to the eventual transition as "CMMC 3.0" though that is not an official term.

**DoD CC SRG (aligned with FedRAMP).** The Cloud Computing SRG continues to align with FedRAMP baselines. IL2 typically requires FedRAMP Moderate; IL4 and IL5 require FedRAMP High plus DoD-specific overlays. Watch for DoD updates on IL5 boundary criteria; the line between IL5 and IL6 (Secret-classified) continues to evolve.

**Continuous Authorization to Operate (cATO).** DoD's cATO model and similar agency efforts continue to shift authorization away from three-year point-in-time renewals toward continuous monitoring evidence streams. SMBs preparing for ATO today should be designing continuous monitoring instrumentation from Day 1; the package format is shifting under everyone.

What this means for you: the return of CMMC third-party assessment, on a date DoD has not yet announced, is the most material upcoming change for defense-facing SMBs; keep the Level 2 self-assessment and annual affirmation current in the meantime. FedRAMP and agency ATO authorization packages are stable on Rev 5 for the immediate future. cATO instrumentation is the forward-looking investment; build for it now even if your first authorization is point-in-time.

# Printable Scoring Sheet

Print this page. Take it to a conference room. Walk through the 28 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 readiness work.

### 1. Governance and Ownership

- ☐ Compliance owner identified _____
- ☐ Security lead assigned _____
- ☐ Technical lead assigned _____
- ☐ Authorization path identified _____
- ☐ Budget allocated _____
- ☐ Executive sponsor engaged _____

### 2. Scope and Boundaries

- ☐ Authorization boundary defined in writing _____
- ☐ In-scope systems and data flows documented _____
- ☐ Shared responsibility model mapped _____
- ☐ Third-party SaaS FedRAMP status verified _____
- ☐ FIPS 199 data classification complete _____
- ☐ Network diagrams current and signed off _____

### 3. Documentation Body

- ☐ SSP current within last 12 months _____
- ☐ Security policies cover all required families _____
- ☐ SOPs documented for key activities _____
- ☐ IR plan tested in last 12 months _____
- ☐ Configuration Management Plan documented _____
- ☐ Contingency Plan / ISCP with test record _____

### 4. Technical Controls

- ☐ MFA enforced for all privileged users _____
- ☐ RBAC with least-privilege; quarterly reviews _____
- ☐ Encryption at rest (FIPS 140-3); TLS 1.2+ _____
- ☐ Audit logging with required retention _____
- ☐ Vulnerability scanning at defined cadence _____
- ☐ Configuration management with drift detection _____

### 5. Evidence Collection and Remediation

- ☐ Evidence collection process defined _____
- ☐ Evidence mapped to control requirements _____
- ☐ POA&M maintained with owners and dates _____
- ☐ Known gaps prioritized and assigned _____
- ☐ Remediation reviewed monthly minimum _____
- ☐ Previous findings addressed and documented _____

**Total implemented (out of 28): _____**

23-28: Strong posture. Engage assessor; instrument continuous monitoring.
15-22: Foundations forming; close gaps via the 90/60/30-day timeline.
Below 15: Significant gaps; start with Section 1 (Governance) and Section 3 (Documentation).

# A Note on Pandora Cloud

Pandora Cloud is a Women-Owned Small Business 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. We help regulated SMBs across defense, healthcare, finance, legal, and insurance build compliant cloud environments and operate them as part of normal business, not as periodic audit projects.

If you scored Yellow or Red and want a second set of eyes on which gaps to prioritize, we offer free 30-minute consultations.

Run the dollar math on a structured 90-day authorization path versus the current trajectory: pandoracloud.net/cost-calculator/. The Cost Calculator includes a Defense scenario built for SBIR Phase 2 and Phase 3 teams.

**Want a second set of eyes on your gaps?**

Schedule a free 30-minute consultation. We will walk through your scored checklist and help you prioritize the next 90 days.

**pandoracloud.net/#schedule-consultation**

# Glossary

For readers new to ATO vocabulary, this glossary names the most common terms used in this checklist.

**ATO (Authority to Operate)**
Formal written authorization issued by an agency Authorizing Official permitting a system to operate at a specified risk level. The output of the Risk Management Framework process.

**AO (Authorizing Official)**
Senior federal official responsible for accepting risk and issuing the ATO. Typically a CIO, CISO, or designated senior executive.

**Body of Evidence (BoE)**
The collection of artifacts (SSP, SAR, POA&M, supporting documents) that an Authorizing Official reviews to make an authorization decision.

**C3PAO (CMMC Third-Party Assessment Organization)**
Organization authorized to perform CMMC Level 2 assessments on behalf of DoD contractors.

**cATO (Continuous Authority to Operate)**
Authorization model that replaces three-year point-in-time renewals with continuous monitoring evidence streams.

**CSP SRG (Cloud Service Provider Security Requirements Guide)**
DoD's set of cloud-specific security requirements layered on top of FedRAMP. Defines Impact Levels IL2 through IL6. Split in June 2024 into a Cloud Service Provider SRG, which governs providers, and a Mission Owner SRG, which governs the DoD components and contractors consuming those services. Current CSP SRG revision: V1R7, 30 June 2026.

**CMMC (Cybersecurity Maturity Model Certification)**
DoD's certification framework for contractors handling FCI or CUI. Three levels (1, 2, 3); Level 2 is the most common for SMB defense contractors.

**ConMon (Continuous Monitoring)**
Ongoing collection of evidence demonstrating that authorized controls remain effective. FedRAMP requires monthly scan reports and quarterly POA&M updates at minimum.

**CUI (Controlled Unclassified Information)**
Federal information that is not classified but requires safeguarding per agency-specific rules. CMMC Level 2 is required for contractors handling CUI under most DoD contracts.

**FedRAMP (Federal Risk and Authorization Management Program)**
Federal program standardizing security assessment for cloud services. Three baselines (Low, Moderate, High) mapped to NIST 800-53 control selections.

**FIPS 199**
Federal Information Processing Standard for security categorization; classifies systems by impact level (Low, Moderate, High) on confidentiality, integrity, and availability.

**FCI (Federal Contract Information)**
Information not intended for public release that is provided by or generated for the government under contract.

CMMC Level 1 covers FCI handling.

**Impact Level (IL)**
DoD CSP SRG categorization: IL2 (public/non-CUI), IL4 (CUI), IL5 (unclassified NSS), IL6 (Secret-classified).

**NIST 800-53**
National Institute of Standards and Technology Special Publication 800-53. The catalog of security and privacy controls for federal systems. Currently at Revision 5.

**NIST 800-171**
Subset of NIST 800-53 controls applicable to non-federal systems handling CUI. Currently at Revision 2 for CMMC; Revision 3 published but not yet adopted.

**P-ATO (Provisional Authority to Operate)**
FedRAMP authorization issued by the Joint Authorization Board (JAB) rather than a single agency. JAB P-ATOs may be reused by every federal agency.

**POA&M (Plan of Action and Milestones)**
Tracked list of known control gaps with owners, target completion dates, and remediation status. Required for ATO; updated continuously post-authorization.

**RMF (Risk Management Framework)**
NIST SP 800-37 process for managing federal information system security risk. Six steps: Categorize, Select, Implement, Assess, Authorize, Monitor.

**SAR (Security Assessment Report)**
Independent assessor's findings document. Reviewed by AO as part of the authorization decision package.

**SSP (System Security Plan)**
Document describing how the system implements its required controls. Written using NIST SP 800-18 guidance; the central artifact in any authorization package.

**3PAO (Third Party Assessment Organization)**
Independent organization accredited to perform FedRAMP security assessments. Selected by the cloud service provider; performs the SAR.