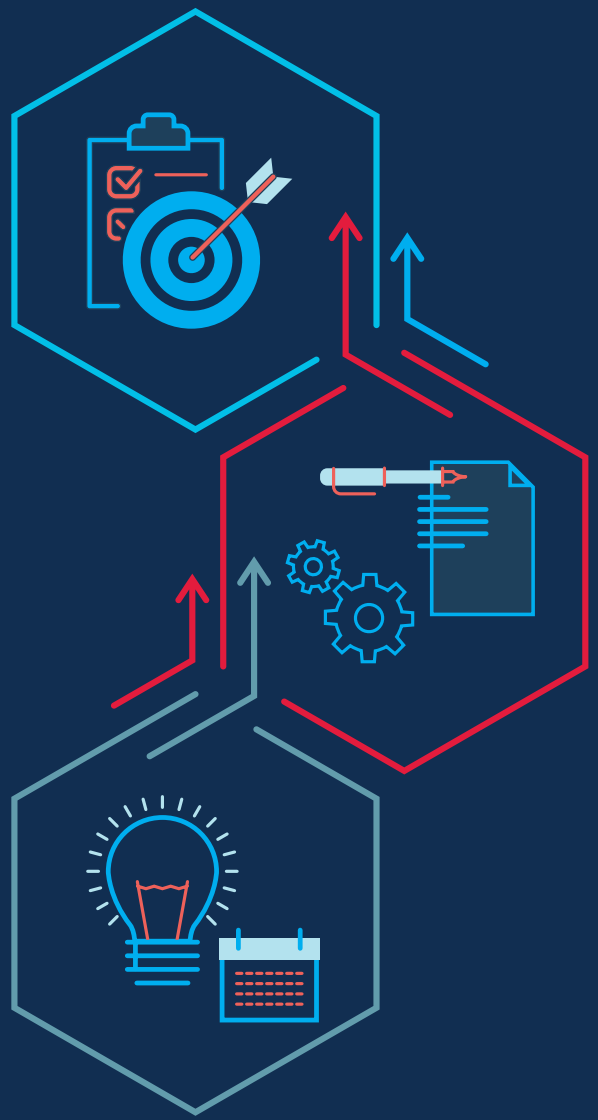
FedRAMP

AGENCY AUTHORIZATION PLAYBOOK



THIS IS THE RECOMMENDED FEDRAMP INITIAL AGENCY AUTHORIZATION PROCESS. THIS PLAYBOOK OUTLINES EACH STEP OF THE PROCESS.

INTRODUCTION

WHY USE FEDRAMP

- Agencies have the opportunity to save money and time by adopting innovative cloud services to meet their critical mission needs.
- Agencies are required by law to protect federal data stored in the cloud. Agencies do this by authorizing cloud services that demonstrate their compliance with one of the FedRAMP security baselines.
- FedRAMP provides a standardized approach to security authorization in accordance with FISMA and NIST security requirements. One of our main goals is to prevent Agencies from reinventing the wheel; the "do once, use many" approach promotes reuse of security assessments to save Agencies time and resources.
- FedRAMP facilitates collaboration across the federal government. We regularly provide guidance and support to help Agencies through the authorization process.
- Email **agency@fedramp.gov** to learn about any upcoming events or new resources available for Agencies.

WHY THIS DOCUMENT

- The purpose of this playbook is to provide Agencies with step-by-step guidance, best practices, and tips to successfully implement the FedRAMP authorization process.
  - » We created this playbook based on best practices from the re-designed FedRAMP Joint Authorization Board (JAB) Provisional Authorization process.
- The overall purposes of this playbook are:
  - » To outline the process for issuing an initial FedRAMP authorization from start to finish.
  - » To promote transparency and consistent expectation management between federal Agencies and Cloud Service Providers (CSPs).

WHAT YOU WILL GET FROM THIS DOCUMENT

- Purpose and outcomes for each step of the process
- Agency, CSP, and Third Party Assessment Organization (3PAO) roles and responsibilities
- Best practices and considerations for working effectively with stakeholders and executing the security review
- FedRAMP resources and templates available for your reference
- Recommended timeframes for each step in the authorization process

HOW TO USE THIS DOCUMENT

- This document was designed as a reference for Agencies pursuing an initial FedRAMP authorization. For information on how to functionally reuse an existing authorization, reference the **Agency Guide for FedRAMP Authorizations.**
- Reference it throughout the process in conjunction with ongoing communication with the FedRAMP Program Management Office (PMO).

FedRAMP

1. PRE AUTHORIZATION

PURPOSE

- For Agencies, the CSP, and the 3PAO to collaborate in preparation for the Agency authorization process

OUTCOMES

- Established relationships with the CSP and the PMO
- Developed plan for authorization

PARTNERSHIP ESTABLISHMENT

PURPOSE

- To select a Cloud Service Offering (CSO) that will meet your Agency mission needs
- To establish working relationships with the CSP, PMO, and other relevant Agencies

OUTCOMES

- Selection of a CSO to move forward with in the FedRAMP authorization process
- FedRAMP PMO is informed of your CSO selection

HOW TO ESTABLISH YOUR PARTNERSHIP

AGENCY'S ROLES AND RESPONSIBILITIES

- Clearly define your Agency's mission needs and specific requirements for a CSO and begin researching possible providers.
- Check the **FedRAMP Marketplace** to see if there is a CSO you are interested in that has already started the process or is authorized. If there is a CSO in the Marketplace that you are interested in, work with the FedRAMP PMO via **info@fedramp.gov** to learn more about their authorization status and package.
- If you are having difficulty selecting a CSO, reach out to **agency@fedramp.gov**. The PMO would be happy to meet with you to discuss your options and share lessons learned from other Agencies.
- Once you have found a CSO that will meet your Agency mission needs, meet with that CSP to determine the feasibility of authorizing their product and keep in mind the organization's willingness and commitment to adhering to federal security requirements.
- Confirm a CSP's dedication to taking on the FedRAMP authorization process. Clearly outline the level of effort involved in the authorization process and your Agency's specific requirements.
- Once you have met with and selected a CSO, send an email to **info@fedramp.gov** sharing your intent to authorize that selected CSO in accordance with FedRAMP's In Process Requirements.

BEST PRACTICES AND CONSIDERATIONS

- Consider your contracting approach early on. A contract between the CSP and Agency does not need to be in place to move forward with the FedRAMP authorization, although there could be.
- Take into account the following considerations when determining the readiness and likelihood for success of a CSP's CSO in the FedRAMP authorization process:
  - » Fully built and functional system
  - » Mature organizational and security processes
  - » Previous experience with federal security authorizations
  - » Committed CSP leadership team

BEST PRACTICES AND CONSIDERATIONS CONTINUED

- Dependencies on other CSOs (including leveraging another hosting provider or external providers that provide functionality)
- Proven maturity (CMMI Level 3+, ISO Organizational Certifications)
- Other certifications (SOC2, ISO27001, PCI)

- Develop an understanding of the cloud architecture/deployment model as soon as possible.
- FedRAMP can act as a conduit between the Agency and CSP to provide an introduction if needed.
- Understand the sensitivity of the data that will be used with the CSO you are considering and ensure the CSO will be able to provide the right level of security given the data. To categorize your data, review the NIST Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

RESOURCES AND TEMPLATES

- Creating Effective Cloud Computing Contracts for the Federal Government (Request from the PMO)
- **Acquisition FAQs**
- **FedRAMP Marketplace Designations for Cloud Service Providers**

AUTHORIZATION PLANNING

PURPOSE

- To plan and set up your FedRAMP Agency authorization for success

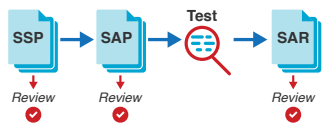
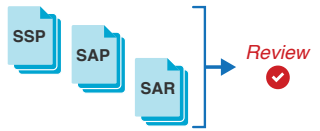
OUTCOMES

- Confirmed resources and authorization project plan to include milestones, schedules, and deliverables
- Clear understanding of authorization roles and responsibilities for all stakeholders (CSP, 3PAO, and Agency)

HOW TO PLAN FOR AN AUTHORIZATION

AGENCY'S ROLES AND RESPONSIBILITIES

- Determine who the Agency Authorizing Official (AO) is. If you need support in identifying and partnering with your Agency's AO, reach out to the FedRAMP PMO.
- Confirm your resources. An Agency should have at least one technical reviewer (TR) (ISSO/ISSM) assigned to the authorization process. The technical reviewer works closely with the CSP to obtain timely answers to questions and with the Agency AO for the final approval and authorization of the Cloud Service Offering.
- Determine your authorization approach. There are two primary methods to successfully complete an authorization:
  1. Just-In-Time Linear Approach
  2. All Deliverables Provided Simultaneously. See the description to the right.
- Identify and provide additional Agency-specific requirements above the FedRAMP security control baseline (if applicable).

Just-In-Time Linear Approach	All Deliverables Provided Simultaneously
	
Each FedRAMP deliverable builds upon another, starting with the SSP. The CSP will complete the SSP + Attachments, SAP, and SAR in a linear fashion, obtaining feedback from the Agency once each deliverable is produced. In turn, the CSP will make modifications to each deliverable, based on the Agency's review. Once the deliverable is finalized and accepted by the Agency, the CSP will begin work on the next deliverable.	All FedRAMP deliverables (SSP + Attachments, SAP, SAR, POA&M) are completed by the CSP and submitted to the Agency by project kick-off. The Agency will review all deliverables at once and work collaboratively with the CSP. This approach resembles how authorizations are completed for a JAB P-ATO.

AGENCY'S ROLES AND RESPONSIBILITIES CONTINUED

- Develop an initial project plan. Map out the various milestones associated with the authorization and provide your notional schedule for CSP and 3PAO input. The FedRAMP PMO is also available to provide feedback on your schedule.
- Contact the PMO at **info@fedramp.gov** for the following:
  c. Request a sample authorization schedule.
  d. Once there is consensus (Agency, CSP, and 3PAO) on the authorization schedule, submit notional authorization dates to the PMO for posting in the **FedRAMP Marketplace**.
  e. Request access to FedRAMP's secure repository. This is where the CSP and 3PAO will upload their documentation.
- Coordinate with the CSP to define Agency/CSP roles and responsibilities. The FedRAMP PMO has developed collateral to assist, see **Agency Authorization Roles and Responsibilities for FedRAMP CSPs and Agencies**.

CSP'S ROLES AND RESPONSIBILITIES

- Confirm resources dedicated to the authorization process. At a minimum this should include 1) one technical writer, 2) one technical SME, and 3) one project manager.
- Work in conjunction with the Agency to select a 3PAO. While CSPs can utilize other independent assessment organizations for Agency ATOs, FedRAMP strongly recommends the use of a **FedRAMP-accredited 3PAO**.
- Possibly engage a consultant for assistance.
- Provide the Agency with updates to notional authorization schedule given resources, time constraints, etc.
- Complete FedRAMP **Training**, including the mandatory training: FedRAMP System Security Plan (SSP) Required Documents (200-A).
- Complete a **FedRAMP CSP Information Form** and receive a package ID number from the FedRAMP PMO.
- Contact the PMO at **info@fedramp.gov** for access to FedRAMP's secure repository.

3PAO'S ROLES AND RESPONSIBILITIES

- Confirm resources dedicated to the authorization process. At a minimum this should include 1) one penetration tester, 2) one technical SME, and 3) one project manager.
- Provide the Agency with updates to the notional authorization schedule given resources, time constraints, etc.

BEST PRACTICES AND CONSIDERATIONS

- Develop a shared understanding of the NIST Risk Management framework within your Agency authorization team. This is the basis of the structure for your authorization schedule.
- The authorization planning process should be a collaborative effort between your Agency, CSP, and 3PAO.
- Have regular and candid discussions with the FedRAMP PMO and the CSP throughout the authorization planning process to ensure that project risk are understood.
- Engage the FedRAMP PMO (**info@fedramp.gov**) when needed to provide clarification of FedRAMP authorization process/procedures.
- A CSP's level of commitment and success exhibited during the authorization planning process is often indicative of their success in the actual process.
- Both the CSP and Agency instance (including Agency responsibilities) portions of the stack should be included in the authorization boundary.
- Face-to-face interactions encourage positive and transparent working relationships among all stakeholder groups.
- The CSP and Agency should strive for consensus. Consensus is not "everyone agrees with everything." Consensus can be defined as: 1) the process for making a decision is explicit, rational, and fair; 2) participants felt they were treated well and their inputs were heard; and 3) participants can live with and commit to the outcomes.
- The process should be agile and collaborative. Don't be afraid to speak up about your concerns in service of meeting the project outcomes. If there are any immediate "showstoppers," it is critical to identify them as early as possible for a timely authorization.

RESOURCES AND TEMPLATES

- CSP FedRAMP Training
- FedRAMP CSP Information Form
- List of FedRAMP Accredited 3PAOs
- Sample Authorization Schedule (Request from the PMO)
- Agency Roles and Responsibilities for FedRAMP CSPs and Agencies

FedRAMP

2. DURING AUTHORIZATION

PURPOSE

- To review the Cloud Service Offering security authorization package

OUTCOMES

- Reviewed Cloud Service Offering documentation including the System Security Plan (SSP), Security Assessment Plan (SAP), and the Security Assessment Report (SAR)
- Approved Cloud Service Offering documentation and testing updates
- Authority to Operate (ATO) decision

KICK-OFF

PURPOSE

- To introduce all team members (3PAO, CSP, Agency) and validate roles and responsibilities
- To kick-off the Agency authorization process

OUTCOMES

- Shared understanding of the Cloud Service Offering, the boundary, any alternative implementations, deviation requests, and other security considerations
- Established working relationships between teams
- Identified immediate next steps to proceed with authorization
- Shared understanding of overall process, milestones, deliverables, roles and responsibilities, and schedule

HOW TO CONDUCT AN AUTHORIZATION KICK-OFF

AGENCY'S ROLES AND RESPONSIBILITIES

- Identify materials from the CSP and 3PAO you would like to review at the kick-off session and ask them to be uploaded via FedRAMP's secure repository ahead of time.
  - » Suggested materials if available at time of kick-off:
    - Readiness Assessment Report
    - SSP Highlights - Network topography, interconnections, system boundary diagram
    - Select controls: AC-2, AC-4, AC-17, CA-1, CM-6, CP-7, CP-9, IA-2(1), IA-2(2), IA-2(3), IA-2(11), IA-2(12), IR-8, RA-5, RA-5(5), RA-5(8), SA-11, SA-11(1), SC-4, SC-7, SC-13
    - Control Implementation Summary (CIS)
    - Security Assessment Plan (SAP)—Testing methodology and sample sizes
    - Security Assessment Report (SAR)—Table 4-1
    - Plan of Action and Milestones (POA&M)
    - Monthly scan results
- Create a kick-off agenda and meeting design. An agenda lays out the order of topics and a meeting design details how those topics will be discussed. A sample kick-off agenda is as follows:
  - » Understand roles and responsibilities of all project team members including Agency, CSP, and 3PAO personnel.
  - » Review project schedule and milestones and gain consensus from all parties.
  - » Ensure that all parties have access to FedRAMP's secure repository to obtain FedRAMP deliverables.
  - » Review network topology, interconnections, and system boundary diagram.
- If there are any additional Agency requirements, gaining consensus on those at this time is key, as well as any other Agency-specific security concerns.

CSP'S ROLES AND RESPONSIBILITIES

- Submit kick-off materials (to be determined ahead of time) at least a week in advance of the kick-off session to allow for adequate review time. This allows the reviewer to develop thoughtful questions ahead of time.
- Have the right people in the room for the conversation including the system owner, project manager, security SMEs, and technical experts.

3PAO'S ROLES AND RESPONSIBILITIES

- Have the right people in the room for the conversation including the testing lead and the penetration tester.
- Be prepared to speak to the results of the testing and associated methodologies.

BEST PRACTICES AND CONSIDERATIONS

MEETING TIPS

- If you need assistance with the kick-off, feel free to invite the FedRAMP PMO to help facilitate.
- Don't let the session be a repeat of what is written in the documentation. It should be an opportunity to tell a story about the security posture of the CSO.
- Clearly define what is considered a "showstopper" to the review process up front.
- Throughout the kick-off, talk to the facilitator if you have any concerns regarding your ability to move forward with a deep dive review of the CSO.
- Talk to the 3PAO and CSP separately to understand their individual perspective of the risk of the system and challenges they encounter.
- Don't be afraid to have separate breakout sessions with just your Agency team throughout the day to allow people to digest their thoughts and privately share concerns without the CSP and 3PAO.
- At the end of the kick-off session, agree to the action plan moving forward and what the Agency reviewer will recommend to decision-makers.

ROLES AND COMMUNICATION

- Commit to open communication and establish communication channels (i.e., what you will communicate, when, how, and to whom).
- Ensure there is a clear understanding of roles and responsibilities for each stakeholder group throughout the review process.
- Require decision points and actions to be time bound with a date-certain outcome. For example, "3PAO to redo penetration testing within 10 business after the kick-off session."

SECURITY REVIEW

- Understand and agree to Agency-responsible controls (customer responsibilities) throughout the documentation.
- Ask the CSP to submit monthly scans throughout the review process to demonstrate their ability to maintain their security posture after the pending initial authorization.

RESOURCES AND TEMPLATES

- FedRAMP Accelerated Kick-Off Briefing Guidance for CSPs (Request from the PMO)
- FedRAMP Accelerated Sample Meeting Summary (Request from the PMO)
- **FedRAMP Authorization Templates**
- **Initial Authorization Package Checklist**

QUALITY & RISK REVIEW

PURPOSE

- To review the CSP's FedRAMP security authorization package (SSP + Attachments, SAP, SAR, PO&AM) for both quality and risk

OUTCOMES

- A deep understanding of the technical makeup and security of the CSO and the ability to determine the level of risk associated with the system
- Agency understands responsibilities associated with "customer-responsible" controls
- Agency provides the CSP with feedback based on their risk analysis to modify the FedRAMP deliverables (documentation and/or testing) (if applicable)

HOW TO PERFORM A QUALITY AND RISK REVIEW

AGENCY'S ROLES AND RESPONSIBILITIES

- Begin your review based on the approach you determined in your Authorization planning phase **(Just-In-Time Linear or All Deliverables Provided Simultaneously, page 6).**
- Understand the impact of the customer implemented control set that you initially agreed upon with the CSP at the kick-off session.
- Review CSP and 3PAO documentation via the FedRAMP secure repository.
- Analyze Agency-specific controls compared to the FedRAMP baseline and address any delta of controls outside of the FedRAMP baseline.
- Review the CSP's monthly scans submissions throughout the quality and review process.
- When assessing the overall quality and risk of the authorization package, check for major issues or concerns in meeting federal requirements (FIPS 140-2 compliance, Level 3 e-Authentication, Multi-Factor Authentication, logical and physical separation for customers). Additionally, look for the following:
  - » SSP
    - Incomplete implementation statements
    - Blank fields
    - Conflicting implementation status
    - Missing or outdated SSP attachments
  - » SAP
    - Blank fields
    - Missing or outdated evidence artifacts
    - Skewed methodology and scope
  - » SAR
    - Conflicting risk levels between SAR Tables 4.1, 5.1, 5.2, 5.3, False Positives, vulnerability scans, and the POA&M
    - The inventory to documented in the SAR (Appendix C,D, and E) needs to matches the scanned inventory
  - » POA&M
    - Missing POA&M dates or dates that are beyond FedRAMP requirements for remediation

CSP'S ROLES AND RESPONSIBILITIES

- Submit the SSP + Attachments and POA&M via FedRAMP's secure repository per the agreed upon schedule.
- Address any questions or comments throughout the process in a timely manner.
- Possibly engage a consultant for assistance.
- Submit monthly scans to the Agency reviewer throughout the quality and risk review phase.

3PAO'S ROLES AND RESPONSIBILITIES

- Submit the SAP and SAR via FedRAMP's secure repository per the agreed upon schedule.
- Address any questions or comments throughout the process.

BEST PRACTICES AND CONSIDERATIONS

- Timely Agency feedback is critical to the overall project schedule. If the Agency reviewer has questions, discuss them with the CSP to understand the associated risk with the CSO.
- Maintain a regular cadence of meetings that include the Agency, CSP, and 3PAO throughout the quality and risk review in order to address Agency questions and concerns in real time. This might include longer in-person working sessions to address specific areas of the system.
- Develop a method for tracking and updating your comments ahead of time including how to theme similar comments and areas of focus.
- Clearly define deadlines by which each section of the authorization package should be reviewed.
- CSP and 3PAO remediation of the system based on reviewer comments can be iterative. Don't forget to be strategic in your approach to remediating comments.
- Keep an open feedback loop with the CSP, 3PAO, and internal Agency stakeholder to capture lessons learned throughout the process to implement into your next Agency authorization.

RESOURCES AND TEMPLATES

- How to Write a Comment (Request from the PMO)
- **SSP + Attachments, SAP, and SAR Templates**
- Authorization Process Tracker (Request from the PMO)

REMEDIATION

PURPOSE

- To address gaps identified by Agency reviewers to ensure the system is at an acceptable level of risk for the Agency
- To provide a defined timeframe (1) to allow the CSP to make system updates and (2) for the 3PAO to perform associated re-testing based on the Agency review (if applicable)

OUTCOMES

- Agency quality and risk review comments and questions are successfully satisfied for the Agency to move forward with the authorization

HOW TO COMPLETE REMEDIATION

AGENCY'S ROLES AND RESPONSIBILITIES

- Define the remediation plan and key measures of success that address all key findings from the quality and risk review up front.
- Provide timely feedback to the CSP so they can ensure updates are made as quickly as possible.
- Be available to address questions throughout the remediation process.
- If applicable, review the delta testing results as they come in so that you're not reviewing all the findings at the end of the process.

CSP'S ROLES AND RESPONSIBILITIES

- Communicate plans for remediation to the Agency and 3PAO.
- Ask questions if you need clarification from the Agency.
- Work closely with the 3PAO to ensure documentation remains in sync and re-testing occurs as needed.

3PAO'S ROLES AND RESPONSIBILITIES

- Perform delta testing as requested by the Agency reviewer and as needed.
- Work closely with the CSP to ensure documentation remains up-to-date.
- Provide clarification to Agency, if requested, regarding system configurations/ vulnerabilities detected.

BEST PRACTICES AND CONSIDERATIONS CONTINUED

- The remediation phase can happen concurrently with the quality and risk review phase.
- Create a clearly defined timeframe for the remediation phase.
- The Agency review of remediation work can happen on an iterative or linear basis depending on Agency reviewer, CSP, and 3PAO preferences.
- Maintain constant communications throughout the remediation process to ensure solutions are addressing Agency reviewer concerns.
- Don't hesitate to reach out to the FedRAMP PMO if you encounter challenges.
- At the end of the remediation phase, have an in-person remediation close-out meeting to review all changes, address questions in real time, and obtain approval.

RESOURCES AND TEMPLATES

- Authorization Process Tracker (Request from PMO)
- CSP Authorization Playbook (Request from PMO)
- How to Write a Comment (Request from PMO)

FINAL REVIEW

PURPOSE

- To provide the final approval of the CSO's FedRAMP authorization package

OUTCOMES

- Authority to Operate (ATO) issued by Agency Authorizing Official
- CSO's authorization package can be leveraged across the federal government

HOW TO OBTAIN A FINAL APPROVAL DECISION

AGENCY'S ROLES AND RESPONSIBILITIES

- Submit the CSO's authorization package to the Agency AO for final approval and issuance of the ATO.
- Use the **FedRAMP ATO Letter Template** when issuing ATO.
- If the AO authorizes the system for use, submit the authorization package to the FedRAMP secure repository.
- Inform the FedRAMP PMO at **info@fedramp.gov** that the CSP's authorization package has been submitted for review.
- Note that Agencies are only issuing an ATO for their Agency's use of that cloud service. It is not a government-wide blanket risk acceptance. Other Agencies that are interested in authorizing the system will review the security deliverables and issue their own ATO through the reuse model.
- Complete the review. Dot all the "i's," cross all the "t's."

CSP'S ROLES AND RESPONSIBILITIES

- Answer any clarifying questions from the Agency AO and/or the FedRAMP PMO during the final review.
- Update documentation as needed.

3PAO'S ROLES AND RESPONSIBILITIES

- Answer any clarifying questions from the Agency AO and/or the FedRAMP PMO during the final review.
- Update documentation as needed.

BEST PRACTICES AND CONSIDERATIONS

- Brief the AO so that she/he can come to an authorization decision. An AO briefing should contain:
  - Overall risk posture and authorization recommendation
  - High to Medium or High to Low risk adjustments
  - Organizational requirements and why they are required
  - Alternative control implementations and why they are necessary
  - Continuous monitoring maturity and progress during the ATO process

BEST PRACTICES AND CONSIDERATIONS CONTINUED

- Have the CSP and 3PAO participate in the AO brief.
- To ensure the CSP's authorization package is complete, refer to the **Agency ATO Review Template** that is leveraged during the FedRAMP PMO's review.
- The FedRAMP PMO will review authorization packages within 1-2 weeks of submission.

RESOURCES AND TEMPLATES

- **Sample ATO letter**
- **Agency ATO Review Template**

FedRAMP

3. POST AUTHORIZATION

PURPOSE

- To perform ongoing security authorization monitoring practices

OUTCOMES

- Set process and procedures for ongoing security authorization monitoring practices
- Ongoing picture of Cloud Service Offering's current risk posture

CONTINUOUS MONITORING

PURPOSE

- To determine next steps for the CSO's FedRAMP authorization including continuous monitoring

OUTCOMES

- Established an ongoing continuous monitoring process

HOW TO INITIATE CONTINUOUS MONITORING

AGENCY'S ROLES AND RESPONSIBILITIES

- Ask the CSP to conduct a monthly meeting to review continuous monitoring deliverables (a high-level report detailing transactions, scans, and POA&M) with all customers, and use this time to share any concerns or questions with the vendor.
- Share expectations and processes for the CSP's annual assessment, significant changes, and onboarding new functionality to the system.
- It is incumbent upon each Agency to review materials and ensure they agree with any changes, deviation requests, scans, etc. and that the risk posture that they agreed to at the time of authorization remains consistent throughout the lifecycle of the system.
- Reach out to the FedRAMP PMO at info@fedramp.gov with any questions regarding specific continuous monitoring vulnerabilities or if you are unable to obtain the information you need.

CSP'S ROLES AND RESPONSIBILITIES

- Submit monthly POA&M, monthly database, operating system, inventory files, and web application raw scan files.
- Submit Deviation Requests and Significant Change Requests as necessary to FedRAMP's secure repository.
- If an incident occurs, the CSP should adhere to US-CERT guidelines.
- Work with Agency AO to coordinate and approve system changes.
- Submit annual assessments to FedRAMP's secure repository.
- Respond to Agency questions and concerns and remediate vulnerabilities as required in the agreed upon timeframe.
- Adhere to CSP's defined continuous monitoring plan (in accordance with control CA-7).

3PAO'S ROLES AND RESPONSIBILITIES

- Perform annual testing as required by the Agency and CSP.
- Respond to Agency questions and concerns in a timely manner.

BEST PRACTICES AND CONSIDERATIONS

- The CSP can apply a mitigation and request a risk adjustment, which would allow the CSP more time to remediate a vulnerability.
- The CSP can seek approvals for a false positive (FP) if a vulnerability is not accurate for the CSP's system.
- The CSP can seek approvals for operational requirements (OR) if a vulnerability is something that a CSP cannot fix, does not plan to fix, or a fix would break the system. CSPs should apply all mitigations possible to lower the risk of the vulnerability prior to requesting an OR. As a note, High risks are typically not approved and must have some mitigation in place to be accepted.
- If a vulnerability cannot be resolved by a CSP directly but is dependent on another vendor to fix, then the CSP should submit this vulnerability as a vendor dependency (VD). A CSP should check in with the vendor at least once a month so the vulnerability is not considered late.
- CSPs are required to perform scanning at least monthly, but it is recommended that vendors scan at least weekly. High and Critical findings must be addressed within 30 days of discovery, and Moderate vulnerabilities must be addressed within 90 days.

RESOURCES AND TEMPLATES

- **FedRAMP Annual Security Assessment Plan (SAP) Template**
- **FedRAMP Annual Security Assessment Report (SAR) Template**
- **FedRAMP New Cloud Service Offering (CSO) or Feature Onboarding Request Template**