FedRAMP

FedRAMP Agency Authorization Playbook

Version 2.0

10/20/2021

GSA

info@fedramp.gov
FedRAMP.gov

Document Revision History

Date	Version	Page(s)	Description	Author
11/28/2017	1.0	All	Initial publication	FedRAMP PMO
10/20/2021	2.0	All	Document updated to provide clarity on updated processes and information	FedRAMP PMO

Table of Contents

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 compliance with one of the FedRAMP security baselines.
- The FedRAMP Policy Memo states that "each Executive department or agency shall use FedRAMP when conducting risk assessments, security authorizations, and granting ATOs [Authorization to Operate] for all Executive department or agency use of cloud services."
- FedRAMP provides a standardized approach to security authorization in accordance with Federal Information Security Modernization Act (FISMA) and National Institute for Science and Technology (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 standardized 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 info@fedramp.gov to learn about any upcoming events or new resources available for agencies.

Why This Document

- This playbook is designed as a reference for agencies pursuing an initial FedRAMP Authorization. For information on how to reuse an existing authorization, reference the Reusing Authorizations for Cloud Products Quick Guide.
- The purpose of this playbook is to provide agencies with guidance, best practices, and tips to successfully implement the FedRAMP authorization process.
- The overall goal of this playbook is to promote transparency and consistent expectation management between federal agencies and Cloud Service Providers (CSPs).
- Reference this playbook throughout the process in conjunction with ongoing communication with the FedRAMP Program Management Office (PMO).

What You Will Get From This Document

- A description of 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

Understanding the FedRAMP Marketplace

The FedRAMP Marketplace provides a searchable, sortable database of Cloud Service Offerings (CSOs) that have achieved a FedRAMP designation. Federal agencies can use the FedRAMP Marketplace to find secure cloud tools that meet their mission needs.

Agencies are encouraged to use the Marketplace as a resource to:

- Research cloud services that are FedRAMP Authorized, or cloud services that are pursuing initial FedRAMP Authorization
- Research agencies that use FedRAMP Authorized cloud services, or agencies that are partnered with CSPs for initial FedRAMP Authorization
- Review FedRAMP's community of accredited 3PAOs

Reusing FedRAMP Authorized Cloud Service Offerings

Cloud Service Offerings that are FedRAMP Authorized are made available for government-wide use. Agencies can leverage the security documentation of a FedRAMP Authorized Cloud Service Offering by following the process outlined in FedRAMP's Reuse Quick Guide.

FedRAMP Designations

FedRAMP defines three different designations for Cloud Service Offerings: FedRAMP Ready, FedRAMP In Process, and FedRAMP Authorized.

- **FedRAMP Ready**: A designation provided to Cloud Service Providers (CSPs) which indicates that a Third Party Assessment Organization (3PAO) attests to a CSO's security capabilities, and that a Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by the FedRAMP PMO. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP Authorization with the Joint Authorization Board (JAB) or a federal agency.
- **FedRAMP In Process**: A designation provided to CSPs that are actively working toward a FedRAMP Authorization with either the JAB or a federal agency. For updates, agencies can either contact the CSP via the email address provided on the CSP's Marketplace page, or reach out directly to the FedRAMP PMO via info@fedramp.gov.
- **FedRAMP Authorized**: A designation provided to CSPs that have successfully completed the FedRAMP Authorization process with the JAB or a federal agency. FedRAMP Authorized service offerings are available for government-wide reuse.

You can learn more about FedRAMP's Marketplace designations by reviewing the FedRAMP Marketplace: Designations for Cloud Service Providers guidance document.

FedRAMP Agency Liaison Program

Program Overview

FedRAMP Agency Liaisons are dedicated points of contact within each agency who serve as the bridge connecting an agency and the FedRAMP PMO. The FedRAMP Agency Liaison Program established a voluntary community of trained individuals that will serve as a unified voice across federal agencies as they teach and facilitate FedRAMP processes and procedures. The goals of the FedRAMP Agency Liaison Program are to promote faster and more efficient authorizations and enable Agency Liaisons to train others within their agencies about the FedRAMP process.

Program Benefits Include:

- **Increased Collaboration** by facilitating a direct line of communications between agencies, bureaus, and the FedRAMP PMO
- **Increased Awareness of FedRAMP** by improving understanding of FedRAMP and the Marketplace throughout the federal government
- **Greater Efficiency** by establishing a single point of expertise that can lead to faster authorizations and less use of resources over time
- **Improved Visibility** to increase transparency into program updates and strategic initiatives

How to Leverage FedRAMP Agency Liaisons

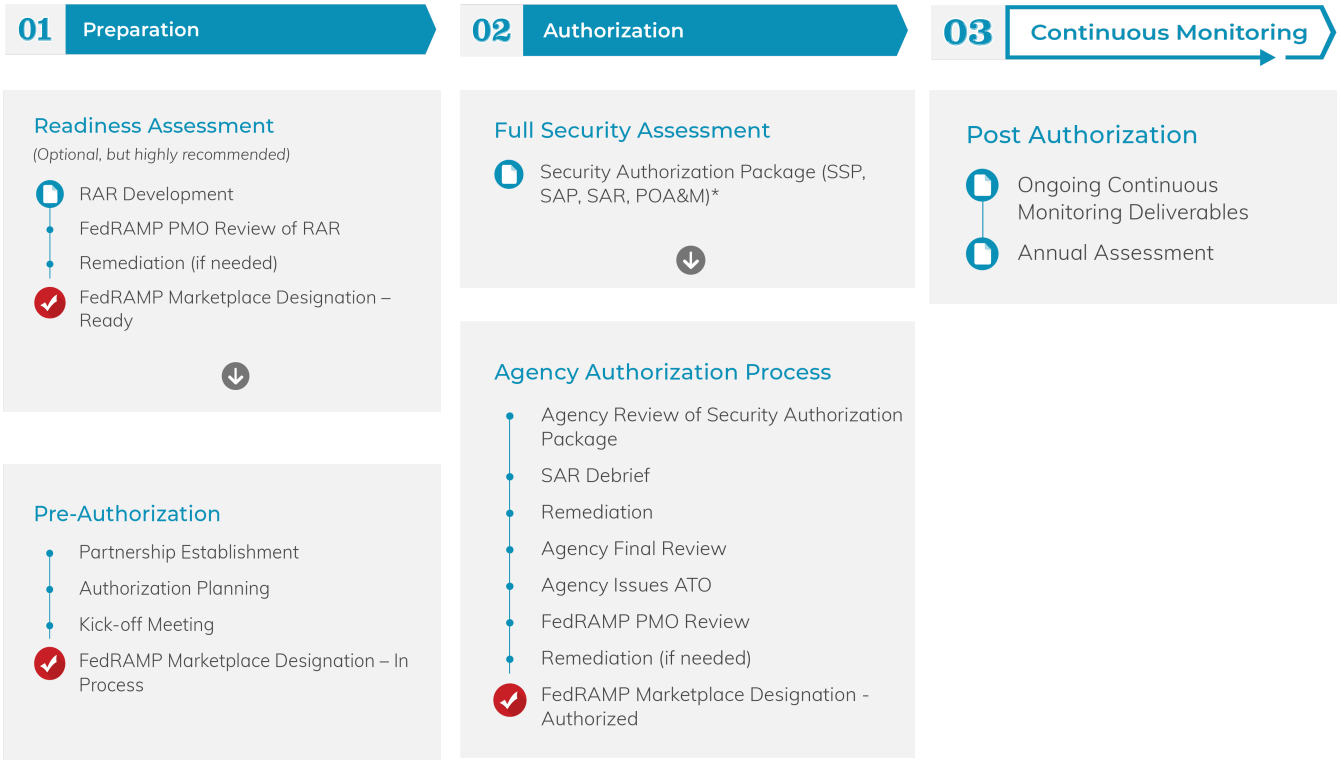
FedRAMP Agency Liaisons can answer general questions about FedRAMP, the FedRAMP reuse process, the Initial Authorization process, and continuous monitoring. Liaisons have been trained to provide seminars and training sessions on these topics within their agencies. In addition, Liaisons can provide information about upcoming training sessions hosted by the FedRAMP PMO.

Liaisons can also provide clarification on the status of cloud vendors within their own agencies, and can help answer questions about how to secure partnership for initial FedRAMP Authorization at their agencies.

Every CFO Act agency has an Agency Liaison who can serve as the subject matter expert and resource for questions about FedRAMP. Many sub agencies and departments have designated their own Liaisons as well. If you are unsure who your Agency Liaison is, please contact info@fedramp.gov. If your agency does not have a Liaison identified, the FedRAMP PMO can help you designate a point of contact and enroll your agency in the program.

Initial FedRAMP Agency Authorization

Below is the recommended FedRAMP initial agency authorization process. The following sections of this playbook outline each step of the process.



** The full security assessment may be prepared in advance of the authorization phase, or completed during the authorization phase. This is dependent on the agency's review approach.*

Partnering for Initial FedRAMP Authorization

Agencies can partner with a CSP for an initial FedRAMP Authorization if they would like to use a CSO that is not currently FedRAMP Authorized. The rest of this playbook explains the initial FedRAMP Authorization process, providing guidance and tips for success at each point along the way.

Common Questions About Partnership

Answers to these frequently asked questions below can be found under the "Federal Agencies" tab of the FAQs page on FedRAMP.gov. If you have additional questions about the responsibility of an initial authorizing agency, please first reach out to your agency's FedRAMP Agency Liaison before reaching out to the PMO at info@fedramp.gov.

What does it mean to be an initial agency partner?

Is there an additional level of effort associated with being the initial authorizing agency?

As the initial authorizing agency, are we responsible for performing Continuous Monitoring (ConMon) oversight on behalf of other leveraging agencies?

Does FedRAMP accept both an Authority to Operate (ATO) and an Authority to Use (ATU)?

What happens if my agency decides to stop using the Cloud Service Offering (CSO)?

What happens if a Cloud Service Offering (CSO) loses its agency customers?

Should my agency use FedRAMP to authorize a private cloud deployment?

Preparation

Readiness Assessment

The FedRAMP Readiness Assessment (known as FedRAMP Ready) is required for CSPs pursuing a JAB Provisional Authority to Operate (P-ATO), and is highly recommended for CSPs pursuing a FedRAMP Authorization with an agency partner. CSOs categorized at the Moderate or High impact levels can achieve a FedRAMP Ready designation.

FedRAMP Ready indicates that a CSP has procured a FedRAMP recognized 3PAO to conduct a readiness assessment, and the 3PAO has determined that the CSP is fully ready to pursue (and likely achieve) a FedRAMP Authorization for the CSO. The results of a readiness assessment are documented in a FedRAMP provided Readiness Assessment Report (RAR) template. The RAR is submitted to the FedRAMP PMO for review and approval. Once approved, the RAR is made available to agencies via MAX.gov.

To understand the scope of a readiness assessment, agencies can review the FedRAMP Moderate RAR template or the FedRAMP High RAR template. At a high level, the Readiness Assessment is primarily focused on the status of technical control implementations versus the status of documentation. While some CSPs may have a fully developed System Security Plan (SSP) at the time of a readiness assessment, a completed SSP is not required. During the readiness assessment, 3PAOs validate the CSP's ability to meet specific federal mandates (e.g. the use of FIPS 140 validated encryption), the CSP's ability to satisfy technical security requirements, and the CSP's maturity in areas such as change management and continuous monitoring.

Agencies should consider partnering with a CSO that has achieved FedRAMP Ready if the CSO meets the agency's mission needs. FedRAMP Ready indicates that the CSP has done most of the heavy lifting and just needs an agency to partner with them on an initial FedRAMP Authorization.

Pre-Authorization

During the pre-authorization phase, the agency and CSP agree to partner on a FedRAMP Authorization. The agency and CSP then work together to prepare for and develop a plan for the agency authorization, and hold a formal Kickoff Meeting.

Partnership Establishment

During the partnership establishment step, the agency agrees to partner with a CSP on an initial FedRAMP Authorization. If you are thinking about partnering with a CSP on an initial FedRAMP Authorization, consider the following steps. If needed, schedule a call with your Agency Liaison or the FedRAMP PMO to talk through the process.

- Clearly define your agency's mission needs and specific requirements for a CSO and begin researching possible providers.
- Understand the sensitivity of the data that will be used with the CSO. To categorize your data, review the NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- Review the FedRAMP Marketplace to see if there is a CSO that meets your mission needs and is able to provide the right level of security given the data. If there is a CSO on the Marketplace that interests you, contact the FedRAMP PMO to learn more about the CSO's authorization status.
- If you find a CSO that meets your mission needs but is not on the Marketplace, meet with that CSP to determine the organization's willingness and commitment to pursue a FedRAMP authorization. If the CSP would like to learn more about the FedRAMP process, direct them to the CSP Authorization Playbook. If the CSP has not already done so, instruct the CSP to complete FedRAMP's CSP Information Form to schedule a preliminary intake call with the FedRAMP PMO.

  Consider the following when determining the CSP's readiness for pursuing a FedRAMP authorization:

  - Fully built and functional system
  - Mature organizational and security processes
  - Committed CSP leadership team
  - Proven maturity (CMMI Level 3+, ISO Organizational Certifications)
  - Other certifications (SOC2, ISO27001, PCI)
  - CSP's ability to meet agency-specific requirements above the FedRAMP security control baseline (if applicable)

- Once you have met with and selected a CSO, review the FedRAMP In Process requirements described in FedRAMP Marketplace Designations for Cloud Service Providers and send the agency In Process Request to info@fedramp.gov. The PMO will provide templates once partnership establishment is confirmed.

Authorization Planning

The purpose of the planning phase is to set up the authorization for success. The authorization planning process is a collaborative effort between the agency and CSP. During the planning phase, stakeholders will:

- Establish a collaborative and transparent working relationship. This includes:
    - Identifying CSP and agency project leads / primary points of contact
    - Deciding how CSP and agency teams will communicate and collaborate. The PMO recommends establishing a recurring meeting (at least bi-weekly) to ensure the project stays on track and that everyone remains accountable for their respective areas of responsibility.
- Determine the agency's approach for reviewing the authorization package as described below:

Just-In-Time Linear Approach	All Deliverables Provided Simultaneously
Each FedRAMP deliverable builds upon another, starting with the SSP. The SSP and attachments, Security Assessment Plan (SAP), and Security Assessment Report (SAR) are completed in a linear fashion, obtaining feedback from the agency once each deliverable is produced. In turn, modifications are made to each deliverable, based on the agency's review. Once the deliverable is finalized and accepted by the agency, work begins on the next deliverable.	All FedRAMP deliverables (SSP and attachments, SAP, SAR, POA&M) are completed and submitted to the agency prior to the Kickoff Meeting. The agency reviews all deliverables at once and works collaboratively with the CSP and 3PAO. This approach resembles how authorizations are completed for a JAB P-ATO.

Helpful Tip: The FedRAMP PMO recommends the Just-In-Time approach as it is a more iterative and agile approach that may prevent rework after 3PAO testing has occurred.

- Identify agency team members assigned to review the authorization package
    - Agency reviewers should have knowledge of the NIST Risk Management Framework and experience reviewing FISMA and/or FedRAMP authorization packages. We highly recommend taking the FedRAMP ISSO on-demand training, which was designed to help agency reviewers understand the process for reviewing a FedRAMP authorization package.
- Determine how the CSP and 3PAO will share authorization package deliverables with the agency
- Develop a method for capturing and tracking agency reviewer comments/questions
- Determine the agency's internal process for reaching an authorization decision and granting an ATO

Kickoff Meeting

The purpose of the Kickoff Meeting is to formally begin the agency authorization process by introducing key team members, reviewing the Cloud Service Offering, and ensuring all stakeholders are aligned on the overall process. While the FedRAMP PMO coordinates and facilitates Kickoff Meetings, Kickoffs are meant to be in service of the CSP and agency partnership. Review FedRAMP's Kickoff Briefing guidance to understand the full scope of a FedRAMP-facilitated Kickoff Meeting.

At the conclusion of the Kickoff Meeting, all stakeholders will have a shared understanding of:

- The overall authorization process, milestones, deliverables, roles and responsibilities, and schedule
- The roles and responsibilities of all project team members including agency, CSP, and 3PAO personnel
- The CSO's purpose and function, authorization boundary, data flows, known security gaps and plans for remediation, agency-specific requirements, customer responsible controls, and areas that may require agency risk acceptance
- The agency's process for reviewing the authorization package and reaching a risk-based authorization decision
- The PMO's process for reviewing the authorization package from the perspective of government-wide reuse
- Best practices and tips for success

Kickoff: Roles and Responsibilities

FedRAMP PMO

Prior to the SAR Debrief:

- Coordinate with the CSP, agency, and 3PAO (optional) to schedule the Kickoff Meeting
- Provide guidance to the CSP to inform the development of a Kickoff Briefing presentation
- Review the completed Kickoff Briefing to verify that all required content is covered
- Remain available to answer any questions leading up to the Kickoff

During the Kickoff:

- Walk through the overall process and milestones
- Describe the PMO's process for reviewing the authorization package
- Describe best practices and tips for success

CSP

Prior to the Kickoff:

- Develop Kickoff Briefing that aligns with the guidance provided by the PMO
- Deliver Kickoff Briefing to PMO for review and feedback
- Participate in planning meeting(s) with the agency to:
    - Understand agency-specific requirements
    - Understand the agency's process for performing a quality and risk review of the authorization package
    - Communicate customer-responsible controls
    - Decide how the CSP and agency teams will communicate and collaborate throughout the process

During the Kickoff:

- Ensure the right team members attend the Kickoff Meeting; while the CSP's leadership/sales team is welcome to attend, it is important to include team members that can describe the security capabilities of the Cloud Service Offering and answer a variety of technical and security questions
- Deliver Kickoff Briefing that aligns with guidance provided by the PMO

Agency

Prior to the Kickoff:

- Participate in planning meeting(s) with the CSP to:
  - Communicate agency-specific requirements
  - Communicate the agency's process for performing a quality and risk review of the authorization package
  - Understand customer responsible controls
  - Decide how the CSP and agency teams will communicate and collaborate throughout the process

Ensure the right team members attend the Kickoff Meeting:

- While the agency business owner is welcome to attend, it is important to include the agency team members that will be responsible for reviewing the authorization package and making authorization decisions

During the Kickoff:

- Raise questions if anything is unclear! Agency team members should walk away from the Kickoff Meeting with a clear understanding of the authorization boundary, how federal data/metadata is protected as it flows through the system, customer-responsible controls, and any security gaps or areas that may require risk acceptance.
- Describe the agency's process for performing a quality and risk review of the authorization package
- Describe the agency's process for reaching an authorization decision and issuing an ATO letter

Helpful Tip: If there are any additional internal administrative requirements, such as uploading to any Governance, Risk Management, and Compliance (GRC) tools, they should be communicated at the Kickoff Meeting and built into the authorization timeline.

Authorization

Full Security Assessment

The CSP is responsible for delivering a security package that is clear, complete, concise, and consistent to adequately describe how they implement security controls for their system using the required FedRAMP Templates. The agency's role in this step of the process is to review the documentation provided by the CSP and provide feedback where deemed necessary. The ultimate goal is for the CSP to provide a security package that other agencies can leverage for review.

During the Full Security Assessment phase, the 3PAO performs an independent audit of the system. Depending on the agency's review approach determined in the Authorization Planning phase, the agency may review and approve the SSP and SAP prior to the start of the 3PAO assessment.

During this step, the 3PAO tests the CSP's system. At the conclusion of testing, the 3PAO develops a Security Assessment Report (SAR) which details their findings from testing and includes a recommendation for FedRAMP Authorization.

The CSP will then develop a Plan of Action and Milestones (POA&M) based on the SAR findings, and include input from the 3PAO, which outlines a plan for addressing the findings from testing.

Agency Authorization Process

Agency Review of Security Authorization Package

During this phase, the agency team conducts a quality and risk review of the CSO authorization package that includes: the System Security Plan (SSP) and attachments, Security Assessment Plan (SAP), Security Assessment Report (SAR), and POA&M.

The purpose of the review is to ensure that the authorization package clearly and accurately reflects the security posture of the CSO in order for the Agency Authorizing Official (AO) to make an informed risk-based authorization decision. A helpful resource is the Agency ISSO on-demand training to help agency reviewers understand the process for reviewing a FedRAMP authorization package.

The PMO recommends establishing 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.

SAR Debrief

The purpose of the SAR Debrief is to help inform the agency's risk review of the CSO. During the SAR Debrief, the 3PAO presents the results of the security assessment, the CSP presents the plan and timeline for remediating residual risk, and the FedRAMP PMO describes the remaining milestones and tips for success. The PMO coordinates and facilitates the SAR Debrief; however, it is meant to be in service of the CSP and agency partnership.

At the conclusion of the SAR Debrief, all stakeholders will have a shared understanding of:

- The 3PAO's assessment approach, methodology, and schedule
- The scope of testing, which includes validation of the authorization boundary and data flows
- The assessment results and residual risk
- The CSP's plan and timeline for remediating residual risk
- Deviation Requests that require agency approval (risk adjustments, false positives)
- Operationally required risks that require agency risk acceptance (for example: services or components essential to the operation of the CSO, but *excluded* from the tested boundary)
- The agency's process for reviewing the authorization package and reaching a risk-based authorization decision
- The PMO's process for reviewing the authorization package from the perspective of government-wide reuse
- Best practices and tips for success

SAR Debrief: Roles and Responsibilities

FedRAMP PMO	
Prior to the SAR Debrief: • Coordinate with the CSP, 3PAO, and agency to schedule the SAR Debrief • Provide guidance to the 3PAO and CSP to inform the development of a SAR Debrief presentation • Review the completed SAR Debrief presentation to verify that all required content is covered • Remain available to answer any questions leading up to the SAR Debrief	**During the SAR Debrief:** • Walk through the remaining milestones and deliverables • Describe the PMO's process for reviewing the authorization package • Describe best practices and tips for success

3PAO and CSP

Prior to the SAR Debrief:

- Provide the final SAR and POA&M to the agency for review at least two weeks prior to the SAR Debrief
- Develop the SAR Debrief presentation that aligns with the guidance provided by the PMO. The 3PAO and CSP will be responsible for separate portions of the presentation.
- Deliver SAR Debrief presentation to PMO for review and feedback
- Ensure the right 3PAO and CSP team members attend the SAR Debrief

During the SAR Debrief:

- Deliver the SAR Debrief presentation and address the agency's questions about the assessment, findings, and plan for remediation

Agency

Prior to the SAR Debrief:

- Review the final SAR and POA&M prior to the SAR debrief meeting and record any questions for the CSP and 3PAO during the meeting

During the SAR Debrief:

- Raise questions if anything is unclear! The agency should walk away from the SAR Debrief with a clear understanding of the scope of testing, the CSP's plan and timeline for remediating any residual risk, and any areas that will require agency risk acceptance.
- Describe the agency's process for completing the quality and risk review of the authorization package, and the process for reaching an authorization decision and granting an ATO

Remediation

To ensure the authorization package clearly and accurately reflects the security and risk posture of the CSO, the CSP and 3PAO may be required to address documentation gaps or inconsistencies identified by the agency review team.

Examples include:

- Inconsistencies across SSP control narratives
- Inconsistencies between the boundary diagram, data flow diagrams, and SSP narrative
- Inconsistencies between control narratives and what is validated by the 3PAO and described in the Security Test Case Procedures workbook
- Inconsistencies between the SAR and POA&M

In addition, the CSP may be asked to remediate or mitigate open risks in order to achieve an acceptable level of risk for the Agency AO.

In some cases, the 3PAO may be required to perform delta testing to validate risk remediations or perform additional testing if the agency review team identifies gaps in the initial assessment scope. For example, if the 3PAO failed to validate the encryption status of federal data/metadata at rest and in transit, or failed to test a component essential to the operation of the CSO.

The agency's review of remediation work can happen on an iterative or linear basis depending on the agency's preference. It is important to maintain constant communication between the agency and CSP throughout the remediation process to ensure that the gaps and other areas of concern are being addressed to the agency's satisfaction.

At the end of the remediation phase, the agency, CSP, and 3PAO should conduct a formal close-out meeting to review all changes, address questions in real time, and obtain approval to move forward to the final review and ATO phase.

Agency Final Review and ATO

During this phase, the agency review team finalizes its review of the authorization package and the Agency AO issues an ATO for the CSO. The FedRAMP PMO provides an ATO letter template that Agency AOs are encouraged to use. The ATO letter is sent to the CSP and info@fedramp.gov.

The process for closing out the review and issuing an ATO varies from agency to agency. The implementation, testing, and documentation of customer controls in the agency's GRC tool typically occurs during this phase, but may occur earlier in the authorization process. As described in the Authorization Planning section, the agency's process and timeline for reaching an authorization decision and issuing an ATO should be defined early in the process and communicated to all stakeholders to manage expectations.

FedRAMP PMO Review

Once the Agency AO issues the ATO letter, the PMO performs a review of the authorization package to determine suitability for government-wide reuse. The scope of the PMO's review includes:

- A quality review to ensure the authorization package clearly and accurately represents the security and risk posture of the CSO. While the initial authorizing agency conducts a quality review of the authorization package, the PMO's review is considered 'a final set of eyes' to ensure uniformity across all packages listed on the FedRAMP Marketplace.
- A risk review to identify weaknesses or deficiencies that must be addressed before the Marketplace status is changed to 'FedRAMP Authorized'

After the ATO letter is received, the following steps are performed to get to a FedRAMP Authorized designation:

1. CSP and 3PAO upload current versions of package deliverables to secure repository (MAX.gov for Low and Moderate packages, to the CSP's repository for High packages)
2. CSP completes and submits FedRAMP Initial Authorization Package Checklist to info@fedramp.gov
3. PMO verifies that all package deliverables are uploaded
4. Package is placed in the PMO Review Team's queue and reviewed in the order they are received
    - Package reviews typically take 10 business days from the start of review, assuming that there are no significant quality issues that may slow down the review
5. PMO review team sends draft Review Report to all stakeholders (CSP, 3PAO, agency)
    - Draft report documents findings identified during PMO's review, and any areas that require clarification
    - PMO coordinates review meeting to walk through findings and clarification requests, as well as plans for remediation by CSP/3PAO
    - Draft report is sent at least one week prior to the meeting
6. CSP/3PAO address findings and resubmits package; notifies the PMO via info@fedramp.gov
7. PMO performs gap review
    - Communicates remaining gaps or recommends authorization to FedRAMP leadership
    - Once approved, Marketplace designation is changed to **FedRAMP Authorized**

Continuous Monitoring

Once a CSO achieves a FedRAMP Authorized designation, the CSP must:

- Continuously monitor the security posture of the CSO
- Provide agencies with information needed to make risk-based decisions about the ongoing authorization of the CSO

The CSP is responsible for ***implementing*** the continuous monitoring processes and tools to maintain an acceptable security posture. Each agency that issues an ATO for a CSO is responsible for **reviewing** the CSP's Continuous Monitoring (ConMon) activities to ensure the security posture remains sufficient for its own use and supports an ongoing authorization. This includes reviewing the monthly POA&M, approving Deviation Requests and significant changes, and reviewing the results of the Annual Assessment.

These activities are described in the FedRAMP Continuous Monitoring Strategy Guide. Please refer to this document for a more in depth overview of these activities.

Collaborative ConMon

The FedRAMP PMO encourages CSPs who have more than one customer agency to streamline the ConMon process and potentially minimize duplicative efforts in a way that helps each agency still perform their due diligence related to ConMon. The PMO developed a recommended Collaborative ConMon approach. This approach is described in the Guide for Multi-Agency Continuous Monitoring. Collaborative ConMon benefits agencies by allowing them to share responsibility for ConMon oversight, and it benefits the CSP by creating a central forum for addressing questions and achieving consensus related to Deviation Requests, Significant Change Requests and the Annual Assessment - versus having to coordinate with each agency separately.

ConMon Best Practices

- **Authorization Planning:** Start talking to the CSP about ConMon early in the process, especially if you have ConMon requirements that exceed FedRAMP's requirements. If you do, you should make the CSP aware of those requirements before authorizing the system.
- **Continuous Monitoring:** Ask the CSP to hold a monthly ConMon meeting. If multiple agencies are using the CSO, ask the CSP to hold a monthly Collaborative ConMon meeting.
    - The meeting should be held at least one week after the monthly ConMon deliverables are submitted. This will give the agency team time to review the deliverables and come to the meeting ready with questions and recommendations for approvals of Deviation Requests or Significant Change Requests.
    - A monthly ConMon meeting agenda might include:

  - Discussion of past due POA&Ms
  - Deviation Requests pending approval
  - Significant Change Requests (planned changes, changes pending approval, status of implementation & testing)
  - Status of Annual Assessment
- **Continuous Monitoring Accountability:** Think about how you will hold the CSP accountable for meeting ConMon requirements. The FedRAMP Continuous Monitoring Performance Guide explains the actions the FedRAMP JAB takes when a JAB-authorized CSP fails to maintain an adequate ConMon capability. The PMO recommends Agency AOs follow a similar approach for ConMon performance.

Use the PMO for Support

The FedRAMP PMO is dedicated to supporting agencies and CSPs through the initial FedRAMP Authorization process. We encourage leveraging your agency's FedRAMP Liaison, as they have a deep knowledge of the FedRAMP process and requirements for partnering with a CSP for an initial FedRAMP Authorization. Our Customer Success Team is also available to address your agency's questions as you consider partnering with a CSP. Please Reach out to us at info@fedramp.gov.