FedRAMP™

FedRAMP® Agency Authorization Playbook

Version 4.0

12/06/2024

GSA®

info@fedramp.gov
FedRAMP.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
11/28/2017	1.0	All	Initial publication	FedRAMP
10/20/2021	2.0	All	Document updated to provide clarity on updated processes and information	FedRAMP
02/15/2024	3.0	All	Updated to add clarity and align with Rev 5 updates made to FedRAMP guidance documents and templates.	FedRAMP
12/06/2024	4.0	All	Updated to align with OMB Memo M-24-15 and removed outdated references	FedRAMP

TABLE OF CONTENTS

Introduction

1.0 Why Use FedRAMP

- Federal agencies have the opportunity to save money and time by adopting innovative cloud services to meet their critical mission needs.
- Federal agencies are required by law to protect federal data stored in the cloud. Federal agencies do this by authorizing cloud services that demonstrate compliance with one of the FedRAMP security baselines.
- FedRAMP provides a standardized approach to security authorization in accordance with Federal Information Security Modernization Act (FISMA) and National Institute for Standards 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 federal agencies time and resources.
- FedRAMP facilitates collaboration across the federal government and regularly provides guidance and support to help federal agencies through the authorization process.
- Email intake@fedramp.gov to learn about any upcoming events or new resources available for federal agencies.

2.0 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 *FedRAMP Reusing Authorizations for Cloud Products Quick Guide*.
- The purpose of this playbook is to provide federal 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 FedRAMP.

3.0 What You Will Get From This Document

- A description of each step of the process
- Federal 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.

Federal agencies are encouraged to use the FedRAMP Marketplace as a resource to:

- Research CSOs that are FedRAMP Authorized, FedRAMP Ready, or FedRAMP In Process
- Research federal agencies that use FedRAMP Authorized CSOs
- Research FedRAMP recognized 3PAOs

Reusing FedRAMP Authorized CSOs

CSOs that are FedRAMP Authorized are made available for government-wide use. Federal agencies can leverage the security documentation of a FedRAMP Authorized CSO by following the process outlined in *FedRAMP's Reusing Authorizations for Cloud Products Quick Guide*.

4.0 FedRAMP Designations

FedRAMP defines three different designations for CSOs: FedRAMP Ready, FedRAMP In Process, and FedRAMP Authorized.

- **FedRAMP Ready**: A designation provided to CSOs, which indicates that a 3PAO attests to a CSO's security capabilities, and that a FedRAMP Readiness Assessment Report (RAR) has been reviewed and deemed acceptable by FedRAMP. FedRAMP Ready indicates a CSO has a high likelihood of successfully completing an initial FedRAMP authorization.
- **FedRAMP In Process**: A designation provided to CSOs that are actively working toward a FedRAMP authorization. For updates, federal agencies can either contact the cloud provider via the email address provided on the CSO's FedRAMP Marketplace page, or reach out directly to FedRAMP via intake@fedramp.gov.
- **FedRAMP Authorized**: A designation provided to CSOs that have successfully completed the FedRAMP authorization process. FedRAMP Authorized CSOs are available for government-wide reuse.

You can learn more about FedRAMP's Marketplace designations by reviewing the "Marketplace Designations" section on the About FedRAMP Marketplace webpage.

FedRAMP Agency Liaison Program

5.0 Program Overview

FedRAMP Agency Liaisons are dedicated points of contact within most federal agencies who serve as the bridge connecting an agency and FedRAMP. 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.

6.0 Program Benefits Include:

- **Increased collaboration** by facilitating a direct line of communications between federal agencies, bureaus, and FedRAMP.
- **Increased awareness of FedRAMP** by improving understanding of FedRAMP and the FedRAMP 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.

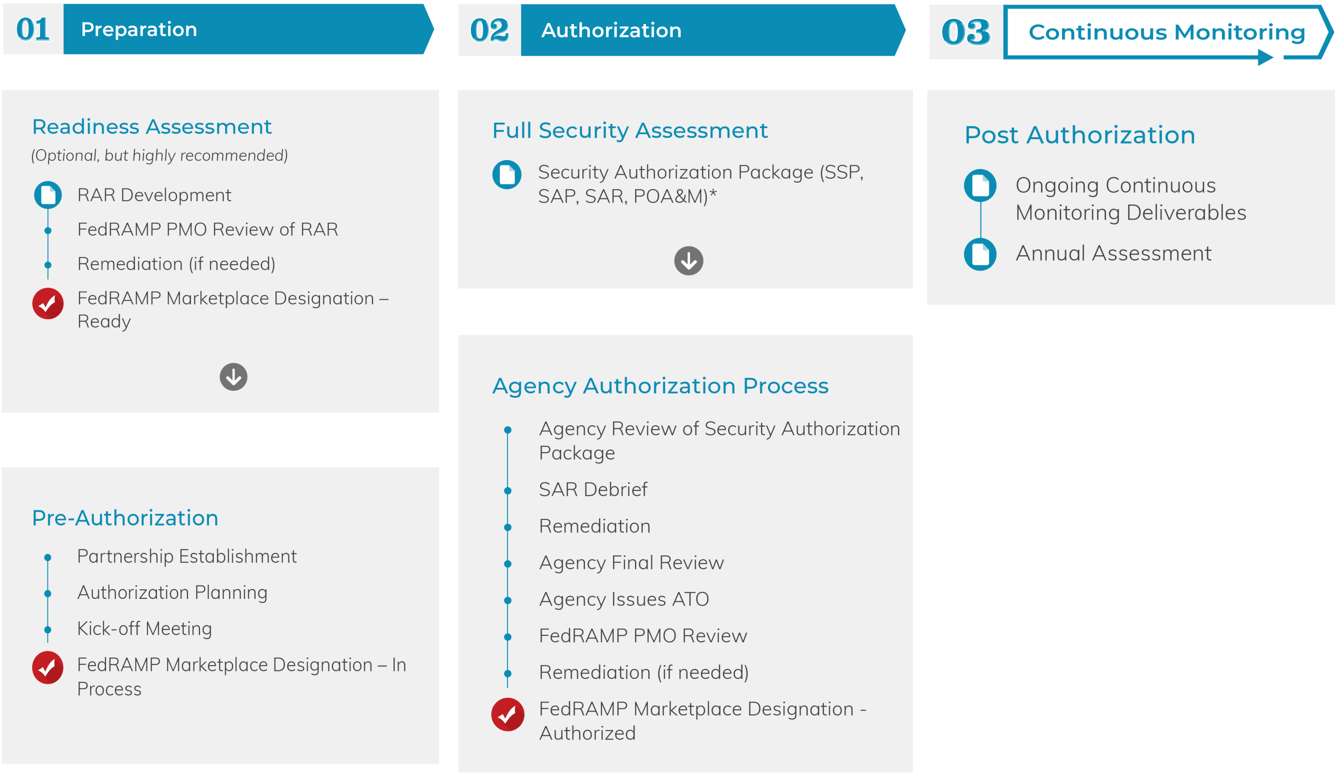
7.0 How to Leverage FedRAMP Agency Liaisons

FedRAMP Agency Liaisons can answer general questions about FedRAMP, the FedRAMP reuse process, the initial authorization process, and continuous monitoring (ConMon). Liaisons attend FedRAMP-hosted meetings to learn about new program initiatives, updated requirements and guidance, and other topics that impact federal agencies. Liaisons can also provide clarification on the status of cloud vendors within their own federal 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 intake@fedramp.gov. If your agency does not have a liaison identified, FedRAMP can help you designate a point of contact and enroll your federal 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.



01 Preparation

Readiness Assessment

(Optional, but highly recommended)

- RAR Development
- FedRAMP PMO Review of RAR
- Remediation (if needed)
- ✓ FedRAMP Marketplace Designation – Ready

Pre-Authorization

- Partnership Establishment
- Authorization Planning
- Kick-off Meeting
- ✓ FedRAMP Marketplace Designation – In Process

02 Authorization

Full Security Assessment

- Security Authorization Package (SSP, SAP, SAR, POA&M)*

Agency Authorization Process

- Agency Review of Security Authorization Package
- SAR Debrief
- Remediation
- Agency Final Review
- Agency Issues ATO
- FedRAMP PMO Review
- Remediation (if needed)
- ✓ FedRAMP Marketplace Designation - Authorized

03 Continuous Monitoring

Post Authorization

- Ongoing Continuous Monitoring Deliverables
- Annual Assessment

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

Partnering for Initial FedRAMP Authorization

Federal agencies can partner with a Cloud Service Provider (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.

8.0 Common Questions About Partnership

Answers to the frequently asked questions below can be found under the "Federal Agencies" section on the FAQs page of FedRAMP's Help Center. 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 FedRAMP at intake@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

9.0 Readiness Assessment

The FedRAMP Readiness Assessment is optional but is highly recommended for CSPs pursuing a FedRAMP authorization with a federal agency partner. CSOs categorized at the Moderate or High impact levels can pursue a FedRAMP Ready designation.

FedRAMP Ready indicates that a CSP has utilized the services of a FedRAMP recognized 3PAO to conduct a FedRAMP Readiness Assessment, and the 3PAO has determined that the CSP is fully ready to pursue (and likely to achieve) a FedRAMP authorization for the CSO. The results of a FedRAMP Readiness Assessment are documented in a FedRAMP provided Readiness Assessment Report (RAR) template. The RAR is submitted to FedRAMP for review and approval. Once approved, the CSO achieves a FedRAMP Ready designation on the FedRAMP Marketplace, and the RAR is made available to federal agencies via the FedRAMP secure repository.

To understand the scope of a FedRAMP Readiness Assessment, federal agencies can review the *FedRAMP Moderate RAR Template* or the *FedRAMP High RAR Template*. At a high level, the FedRAMP Readiness Assessment is primarily focused on the status of technical capabilities versus the status of documentation. While some CSPs may have a fully developed system security plan (SSP) at the time of the assessment, a completed SSP is not required. During the FedRAMP 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 ConMon.

Federal agencies should consider partnering with a CSO that has achieved the FedRAMP Ready designation if the CSO meets the federal agency's mission needs. FedRAMP Ready indicates that the CSP has done most of the heavy lifting and just needs a federal agency to partner with them to pursue an initial FedRAMP authorization.

10.0 Pre-Authorization

During the Pre-Authorization phase, the federal agency and CSP agree to partner on a FedRAMP authorization. The federal agency and CSP then work together to prepare for and develop a plan for the agency authorization and hold a formal kickoff meeting.

10.1 Partnership Establishment

During the Partnership Establishment phase, the federal agency agrees to partner with a CSP to pursue an initial FedRAMP authorization. If you are thinking about partnering with a CSP, consider the following steps, and, if needed, schedule a call with your FedRAMP Agency Liaison to talk through the process:

- Clearly define your federal 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 you find a CSO that meets your mission needs, but is not on the FedRAMP Marketplace, meet with the associated 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 FedRAMP CSP Authorization Playbook. If the CSP has not already done so, instruct the CSP to complete FedRAMP's CSP Information Form. Completing the form will generate a unique FedRAMP ID for the system and provide valuable resources in an automated follow-up email.

  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, etc.)

10.2 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 federal agency and CSP. During the Planning phase, stakeholders will:

Establish a collaborative and transparent working relationship. This includes:

- Identifying CSP and federal agency project leads/primary points of contact.
- Deciding how CSP and federal agency teams will communicate and collaborate. FedRAMP 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.
- Identify federal agency team members assigned to review the authorization package.
    i. Federal agency reviewers should have knowledge of the NIST Risk Management Framework and experience reviewing FISMA and/or FedRAMP authorization packages.
- Determine how the CSP and 3PAO will share authorization package deliverables with the federal agency.
- Develop a method for capturing and tracking agency reviewer comments/questions.
- Determine the federal agency's internal process for reaching an authorization decision and granting an ATO.
- Determine the federal 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 appendices, security assessment plan (SAP), and security assessment report (SAR) are completed in a linear fashion, obtaining feedback from the federal agency once each deliverable is produced. In turn, modifications are made to each deliverable, based on the federal agency's review. Once the deliverable is finalized and accepted by the federal agency, work begins on the next deliverable.	All FedRAMP deliverables (i.e., SSP/appendices, SAP, SAR, and Plan of Action and Milestones (POA&M)) are completed and submitted to the federal agency at once. The federal agency reviews all deliverables together and works collaboratively with the CSP and 3PAO.

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

10.3 Work Breakdown Structure and In Process Request

As your federal agency finalizes the Authorization Planning phase, complete the following actions:

1. Complete a Work Breakdown Structure (WBS) and submit a FedRAMP In-Process Request to FedRAMP via intake@fedramp.gov. The completion of this form indicates to FedRAMP that your federal agency is ready to begin coordinating a kickoff meeting with the CSP and 3PAO (optional and recommended). It also indicates that you have reviewed and approved the WBS, and 3PAO testing is scheduled within six (6) months. At this point, FedRAMP will provide a copy of the kickoff meeting presentation template to the CSP.

2. Instruct your CSP to begin working on the kickoff meeting presentation. A copy of the CSP's completed presentation must be sent to FedRAMP via intake@fedramp.gov for review and feedback prior to confirming a date and time for the kickoff meeting.

See the FedRAMP In Process section on the About FedRAMP Marketplace webpage for more information about the FedRAMP In Process request, WBS, and the full criteria for a CSP to be listed as In Process. Your federal agency's FedRAMP Liaison will be able to assist in the actions listed above.

10.4 Kickoff Meeting

The purpose of the kickoff meeting is to formally begin the FedRAMP agency authorization process by introducing key team members, reviewing the CSO, and ensuring all stakeholders are aligned on the overall process. 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 federal agency, CSP, and 3PAO personnel.
- The CSO's purpose and function, authorization boundary, data flows, known security gaps and plans for remediation, federal agency-specific requirements, customer responsible controls, and areas that may require federal agency risk acceptance.
- The federal agency's process for reviewing the authorization package and reaching a risk-based authorization decision.
- Best practices and tips for success.

Kickoff: Roles and Responsibilities

FedRAMP

Prior to the kickoff meeting:

- Provide guidance to the CSP to inform the development of a kickoff meeting presentation.
- Review the completed kickoff meeting presentation to verify all required content is covered.
- Remain available to answer any questions leading up to the kickoff meeting.

CSP

Prior to the kickoff meeting:

- Develop kickoff meeting presentation that aligns with the guidance provided by FedRAMP.
- Deliver kickoff meeting presentation to FedRAMP for review and feedback.
- Participate in planning meeting(s) with the federal agency to:
  - Understand the federal agency's process for performing a quality and risk review of the authorization package.
  - Communicate customer-responsible controls.

During the kickoff meeting:

- 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 CSO and answer a variety of technical/security questions.
- Deliver kickoff meeting presentation that aligns with guidance provided by FedRAMP.

- ○ Decide how the CSP and federal agency teams will communicate and collaborate throughout the process.

Agency

Prior to the kickoff meeting:

- Participate in planning meeting(s) with the CSP to:
  - Communicate the federal agency's process for performing a quality and risk review of the authorization package.
  - Understand customer-responsible controls that must be implemented and tested by the federal agency.
  - Decide how the CSP and federal agency teams will communicate and collaborate throughout the process.

Ensure the right team members attend the kickoff meeting:

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

During the kickoff meeting:

- Raise questions if anything is unclear. Federal 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 CSO, customer-responsible controls, and any security gaps or areas that may require risk acceptance.
- Describe the federal agency's process for performing a quality and risk review of the authorization package.
- Describe the federal 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

11.0 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 federal 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 federal agencies can leverage for review.

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

During this step, the 3PAO tests and validates the CSP's implementation of security controls, validates vulnerability scans, and performs penetration testing. At the conclusion of the assessment, the 3PAO develops a SAR, which documents the results of the security assessment and includes a recommendation for FedRAMP authorization.

The CSP will then develop a POA&M based on the SAR findings. The POA&M documents the CSP's plan and timeline for remediating residual risk that remained at the conclusion of the security assessment.

12.0 Agency Authorization Process

12.1 Agency Review of Security Authorization Package

During this phase, the federal agency team conducts a review of the CSO authorization package that includes: the SSP and appendices, SAP, 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 federal agency authorizing official (AO) to make an informed risk-based authorization decision.

FedRAMP recommends establishing a regular cadence of meetings that include the federal agency, CSP, and 3PAO throughout the quality and risk review in order to address federal agency questions and concerns in real time. This might include longer in-person working sessions to address specific areas of the CSO.

12.2 SAR Debrief

The purpose of the SAR debrief is to help inform the federal 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 partnering agency describes the remaining milestones and tips for success. 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 federal agency approval (e.g., risk adjustments and false positives).
- Operationally required risks that require federal agency risk acceptance (e.g., services or components essential to the operation of the CSO, but *excluded* from the tested boundary).
- The federal agency's process for reviewing the authorization package and reaching a risk-based authorization decision.
- FedRAMP'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

Prior to 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.

3PAO and CSP

Prior to the SAR Debrief:

- Provide the final SAR and POA&M to the federal agency for review at least two (2) weeks prior to the SAR debrief.
- Develop the SAR debrief presentation that aligns with the guidance provided by FedRAMP. The 3PAO and CSP will be responsible for separate portions of the presentation.
- Deliver SAR debrief presentation to FedRAMP 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 federal 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 federal 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 federal agency risk acceptance.
- Describe the federal 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.

12.3 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 federal 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 FedRAMP 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 federal agency AO.

In some cases, the 3PAO may be required to perform delta testing to validate risk remediations or perform additional testing if the federal agency review team identifies gaps in the initial assessment scope, e.g. 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 federal agency's review of remediation work can happen on an iterative, or linear basis, depending on the federal agency's preference. It is important to maintain constant communication between the federal agency and CSP throughout the remediation process to ensure that the gaps and other areas of concern are being addressed to the federal agency's satisfaction.

At the end of the Remediation phase, the federal 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.

12.4 Agency Final Review and ATO

During this phase, the federal agency review team finalizes its review of the authorization package, and the federal agency AO issues an ATO for the CSO. FedRAMP provides an ATO letter template that federal 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 federal agency to agency. The implementation, testing, and documentation of customer controls in the federal agency's GRC tool typically occurs during this phase, but may occur later in the authorization process after the ATO for the CSO is issued. As described in the Authorization Planning section, the federal 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.

12.5 FedRAMP Review

Once the federal agency AO issues the ATO letter, FedRAMP performs a review of the authorization package to determine suitability for government-wide reuse. The scope of FedRAMP'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, FedRAMP's review is considered 'a final set of eyes' to ensure uniformity across all packages listed on the FedRAMP Marketplace.
- A security review to ensure compliance with FedRAMP requirements and standards.
- A risk review to identify weaknesses or deficiencies that must be addressed before the FedRAMP 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 the FedRAMP secure repository for Low and Moderate packages, or to the CSP's repository for High packages.
2. CSP completes and submits *FedRAMP Initial Authorization Package Checklist* to info@fedramp.gov.
3. FedRAMP verifies that all package deliverables are uploaded.
4. Package is placed in the FedRAMP review team's queue; packages are reviewed in the order they are received.
5. The FedRAMP review team sends draft review report to all stakeholders (CSP, 3PAO, and federal agency).
    - Draft report documents' findings are identified during FedRAMP's review and any areas that require clarification.

  - FedRAMP coordinates a review meeting to walk through findings and clarification requests, as well as plans for remediation by the CSP/3PAO.
  - Draft report is sent at least one week prior to the meeting.

6. CSP/3PAO address findings and resubmits package; notifies FedRAMP via pmo-review@fedramp.gov.
7. FedRAMP performs gap review.
   - Communicates remaining gaps or recommends authorization to FedRAMP leadership.
   - Once approved, FedRAMP Marketplace designation is changed to **FedRAMP Authorized**

Continuous Monitoring

Throughout the Authorization phase, CSPs are required to maintain the system, which includes performing ConMon activities. The CSP's ability to demonstrate a mature ConMon process is one of the areas evaluated during the 3PAO's assessment and during the federal agency and FedRAMP's review of the authorization package. Failure to demonstrate a mature ConMon process will prevent or delay a FedRAMP Authorized designation.

Once the Authorization phase is complete and the CSO achieves a FedRAMP Authorized designation, the CSP:

- Continuously monitors the security posture of the CSO.
- Provides federal agencies with information needed to make risk-based decisions about the ongoing authorization of the CSO.

The CSP is responsible for ***implementing*** the ConMon processes and tools to maintain an acceptable security posture. Each federal agency that issues an ATO for a CSO is responsible for ***reviewing*** the CSP's 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/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.

13.0 Collaborative ConMon

CSPs with more than one federal agency customer are required to implement a collaborative ConMon approach, intended to streamline the ConMon process and potentially minimize duplicative efforts in a way that helps each federal agency still perform their due diligence related to ConMon. This approach is described in the FedRAMP Collaborative ConMon Quick Guide. Collaborative ConMon benefits federal 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 federal agency separately.

13.1 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. As additional federal agency customers begin 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 federal 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 (i.e., planned changes, changes pending approval, and status of implementation and 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 Management Guide provides recommended actions the agency AO may take when a FedRAMP Authorized CSP fails to maintain an adequate ConMon capability. Section 3 of this guide also provides recommendations for processes that federal agencies should use to perform oversight of CSOs authorized via the FedRAMP agency authorization path.

Use FedRAMP for Support

FedRAMP is dedicated to supporting federal agencies and CSPs through the initial FedRAMP authorization process. FedRAMP encourages leveraging your federal 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. FedRAMP's customer success team is also available to address your federal agency's questions as you consider partnering with a CSP. Please reach out to FedRAMP at info@fedramp.gov.