CSP Authorization Playbook

Version 2.0

01/18/2022

GSA

info@fedramp.gov

fedramp.gov

DOCUMENT REVISION HISTORY

Date	Version	Page(s)	Description	Author
07/01/2018	1.0	All	Published Volume 1 of the CSP Authorization Playbook	FedRAMP PMO
01/18/2022	2.0	All	Updated Volume 1 for accuracy and added Volume 2 to the CSP Authorization Playbook	FedRAMP PMO

TABLE OF CONTENTS

VOLUME I: GETTING STARTED WITH FEDRAMP

Getting Started: Is FedRAMP Right For You?

If you have a Cloud Service Offering (CSO) that is being used by the federal government, you should consider obtaining a FedRAMP Authorization. Per an Office of Management and Budget (OMB) memorandum, cloud services that hold federal data must be FedRAMP Authorized.

There are two approaches to obtaining a FedRAMP Authorization: a provisional authorization through the Joint Authorization Board (JAB) or an authorization through an agency. Both authorization paths require a security assessment based on Federal Information Security Management Act (FISMA) requirements and National Institute of Standards and Technology (NIST) 800-53 baselines, and both are explained in greater detail in their respective sections of this document.

In making a business decision regarding the type of FedRAMP Authorization that is most suitable for your service, it is important to consider your overall strategy for federal government customers. If you are brand new to the federal landscape, there may be a learning curve associated with the procurement timeline, and you might want to consider partnering with a systems integrator who has experience and a federal government customer base. Conversely, if you already have a federal government footprint and are looking to expand, a FedRAMP Authorization can be a business development driver. FedRAMP provides cross-government visibility on the FedRAMP Marketplace and provides a single security package that can be leveraged by multiple federal agencies for review.

In addition to the OMB mandate, other drivers for attaining a FedRAMP Authorization are:

- You have an interest in selling your CSO to the federal government.
- Your current federal government customers are asking you to obtain a FedRAMP Authorization.
- You are looking to expand the federal customer footprint by having the ability to market your service as FedRAMP Authorized.

It is also important to understand your CSO's and organization's preparedness and viability for the FedRAMP Authorization process. A Cloud Service Provider (CSP) should be prepared to demonstrate whether its service is operational or is under development and the extent of the current demand for the service in the federal market.

General information including resources, blogs, templates, and documentation for authorization can be found on FedRAMP's website.

Partners in the Authorization Process

1.0 FedRAMP Program Management Office (PMO)

Responsible for providing a unified process to stakeholders, the FedRAMP PMO is a key partner for CSPs researching or seeking a FedRAMP Authorization for their CSO. Its responsibilities include: stewardship of the FedRAMP Authorization process, coordination with the JAB to prioritize vendors to achieve a JAB Provisional Authorization to Operate (P-ATO), project management support for CSPs and agencies; and enabling services to be reused across the federal government by providing a secure repository of FedRAMP Authorizations.

2.0 Joint Authorization Board (JAB)

The JAB is the primary governance and decision-making body for FedRAMP. The JAB is composed of the Chief Information Officers (CIOs) of the Department of Homeland Security (DHS), the General Services Administration (GSA), and the Department of Defense (DoD). The JAB defines and establishes the FedRAMP baseline security controls and the accreditation criteria for Third Party Assessment Organizations (3PAOs). The JAB works closely with the FedRAMP PMO to ensure that FedRAMP baseline security controls are incorporated into consistent and repeatable processes for security assessments and authorizations of CSOs.

CSPs that make a business decision to pursue a JAB P-ATO for their CSO are prioritized through FedRAMP Connect. During this prioritization process, the JAB aims to authorize cloud services it believes are most likely to be leveraged government-wide. This is covered in more detail in FedRAMP's JAB Prioritization Criteria. For CSOs that achieve a P-ATO, the JAB also ensures those systems maintain an acceptable risk posture through Continuous Monitoring (ConMon).

3.0 Federal Agencies

CSPs that make a business decision to work directly with an agency to pursue an Authorization to Operate (ATO) will partner with the agency throughout the initial FedRAMP Authorization process. Agencies define their specific policies and procedures in addition to FedRAMP requirements and are responsible for reviewing CSP-developed security packages. Ultimately, an agency's Authorizing Official (AO) must accept the risk associated with the use of a cloud system through the issuance of an ATO for their agency. Agencies should also conduct Continuous Monitoring oversight of each authorized system in use, reviewing monthly and annual deliverables provided by CSPs.

3.1 Agency Authorizing Official

An agency's AO is a senior federal official who is ultimately responsible for making a risk-based decision to grant a CSP's offering an ATO. The decision is formalized in an ATO letter provided to the CSP system owner and FedRAMP PMO. AOs have sufficient visibility across their organization to understand the impact and cost of an individual CSO on the security environment and operations of the agency.

> **NOTE: The initial agency ATO is not a government-wide risk acceptance. Likewise, the initial authorizing agency is not responsible for performing ConMon oversight on behalf of all federal agencies.** Each agency must issue an ATO for its own use of the CSO and review ConMon deliverables to ensure the security posture remains sufficient for the agency's continued use. CSPs with multiple agency customers should establish a collaborative approach to Continuous Monitoring.

4.0 Third Party Assessment Organizations (3PAOs)

As independent third parties, 3PAOs perform initial and periodic assessments of cloud systems to ensure they meet FedRAMP requirements. CSPs pursuing a FedRAMP Authorization must have their CSOs assessed by an independent third party. For the JAB Authorization process, a CSP must choose a FedRAMP recognized 3PAO that meets the necessary quality, independence, and FedRAMP knowledge requirements to perform required independent security assessments. For the Agency Authorization process, most assessments are conducted using a FedRAMP-recognized 3PAO. However, an agency may choose to use their Independent Verification and Validation (IV&V) organization to assess a CSO. While conducting an initial assessment, assessors are responsible for developing a Security Assessment Plan (SAP) and Security Assessment Report (SAR). FedRAMP-recognized 3PAOs can be found on the FedRAMP Marketplace.

> **NOTE:** If an agency elects to use its own IV&V team or a third-party assessor that is not a FedRAMP-recognized 3PAO, the agency AO must attest to the independence of the assessment organization. In addition, the assessment organization must use FedRAMP-provided templates.

Determining Your Authorization Strategy

There are two approaches to obtaining a FedRAMP Authorization, a provisional authorization through the Joint Authorization Board (JAB) or an authorization through an agency. We recommend that you evaluate the factors below to determine your authorization strategy. Before finalizing a FedRAMP Authorization strategy, the PMO recommends CSPs participate in an intake call with our technical and federal government SMEs for a consultation. CSPs can sign up for an intake call by filling out the CSP intake form.

5.0 Demand: Broad vs. Niche

Demand is a key consideration for CSPs deciding between pursuing a JAB P-ATO or ATO from an agency partner. FedRAMP generally evaluates CSOs as having broad or niche demand. Broad *demand* reflects proven or potential demand for an offering from multiple agencies, and *niche demand* reflects agency-specific utility or applicability of an offering. When evaluating which authorization to pursue, a CSP should be able to qualify whether their offering has broad or niche demand, as CSOs with broad demand are more appropriate for a JAB P-ATO, and CSOs with niche demand are more appropriate for an agency ATO.

> **NOTE:** Broad demand is considered a go/no-go criterion for prioritization of CSOs for a JAB Authorization. CSPs are required to prove current or potential federal demand for their offering(s) by providing one or more of the following: (1) listing of current federal government customers; (2) listing of relevant federal government Request for information (RFI)/Request for Proposal (RFP)/Request for Quotation (RFQ) data; (3) verification from on-premise customers indicating interest in transitioning the service to the cloud; (4) communications from federal government points of contact expressing potential interest; or (5) proof of current state, local, tribal, and territorial customers.

6.0 Existing or Potential Agency Partners

The first step in achieving a FedRAMP Agency Authorization is for a CSP to establish a partnership with a federal agency. Some CSPs may already have an agency or agencies that are interested in authorizing their CSO, because they are either already using the system or they are using an on-premise version and wish to transition to a cloud version. Other CSPs may have potential customers who are interested in their service or may be responding to Requests for Proposals (RFPs) that include FedRAMP requirements. It is critical to discuss FedRAMP early in the process. The PMO can partner with CSPs in discussions with agencies to address questions or concerns about the authorization process.

Common Agency Questions About Partnership

Below are answers to frequently asked questions, which can be found on the "Federal Agencies" tab of the FAQ page on fedramp.gov. As a CSP, it is beneficial to review these and other FAQs on our website to help in your preparedness when these topics arise with agency customers.

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?

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?

7.0 Deployment Model

CSPs should qualify whether their CSO is government-only community, public, or private or exists as a hybrid cloud. FedRAMP adheres to NIST SP 800-145 definitions when defining cloud deployment models.

	Definition
Government-Only Community	The cloud holds only government data. Customers can be federal, state, local, tribal, territorial, federally funded research centers (FFRDCs), contractors working on behalf of the government, or lab entities.
Public	Public cloud deployments support both government and non-government customers. This aligns with the traditional model of cloud computing services, but it potentially poses more of a risk to the federal government.
Private	Private cloud deployments intended for single organizations and implemented fully within federal facilities are not subject to the FedRAMP mandate, and are the only exception to FedRAMP being mandatory for all federal agencies. For private clouds deployed in an IaaS/PaaS versus within a federal facility, the agency should use the FedRAMP process and baselines to authorize the cloud service. However, the FedRAMP PMO does not review packages for private clouds, grant a FedRAMP Authorized designation, or list them on the Marketplace because the concept of "reuse" does not apply.
Hybrid	Combination of cloud infrastructures (private, community, or public). Each cloud is a unique entity but is bound to other clouds to provide services to an organization (e.g., cloud bursting for load balancing between clouds).

8.0 Impact Levels

Federal Information Processing Standard (FIPS) 199 provides the standards for categorizing information and information systems, which is the process CSPs use to ensure their services meet the minimum security requirements for processing, storing, and transmitting federal data. The security categories are based on the potential impact that certain events would have on an organization's ability to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

It is important that CSPs understand the impact level of their service offering(s) and corresponding security categorization when developing an authorization strategy. CSOs are categorized into one of three impact levels (low, moderate, and high) and across three security objectives (confidentiality, integrity and availability).

8.1. Impact Levels

	Definition
Low Impact Levels	The low-impact level is most appropriate for CSOs for which the loss of confidentiality, integrity, and availability would result in limited adverse effects on an agency's operations, assets, or individuals. FedRAMP currently has two baselines for systems with low-impact data: LI-SaaS Baseline and Low Baseline. The LI-SaaS Baseline accounts for low-impact SaaS applications that do not store personal identifiable information (PII) beyond what is generally required for login capability (i.e., username, password, and email address). Required security documentation is consolidated, and the requisite number of security controls needing testing and verification are lowered relative to a standard Low Baseline authorization. Additional information on requirements for the LI-SaaS Baseline can be found on the FedRAMP Tailored website.
Moderate Impact Levels	Moderate-impact level systems account for nearly 80% of CSP services that receive FedRAMP Authorization. It is most appropriate for CSOs for which the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical.
High Impact Levels	High-impact data is usually in law enforcement and emergency services systems, financial systems, health systems, and any other system for which loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. FedRAMP introduced the High Baseline to account for the federal government's most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and against financial ruin..

Additional information on security controls involved in the High, Moderate, Low baselines can be found within the FedRAMP Security Controls Template.

NOTE: CSPs must correctly align their CSOs to an impact level to pursue the appropriate FedRAMP baseline and authorization type. For example, CSOs that qualify for LI-SaaS or align with the Low Baseline cannot obtain a JAB P-ATO, as the JAB only authorizes Moderate and High systems. CSPs should use the FedRAMP FIPS 199 Categorization Template (embedded as Attachment 10 in the SSP) along with the guidance of NIST Special Publication 800-60 volume 2 Revision 1 to correctly categorize their system based on the types of information processed, stored, and transmitted.

Ultimately, the security impact level of a system is determined by the agency customer as each Authorizing Official (AO) will have different risk tolerance levels and each agency's mission is different, which may impact how they classify their data. For this reason, it is important for CSPs to coordinate with their agency customers to ensure agreement with their impact level classification.

8.2. Security Objectives

	Definition	Example
Confidentiality	Information access and disclosure includes means for protecting personal privacy and proprietary information.	Access to John Doe's personal information is sufficiently restricted for the purpose of privacy.
Integrity	Stored information is sufficiently guarded against modification.	Susan Smith lacks the appropriate access and cannot modify John Doe's security information
Availability	Timely and reliable access to information is ensured.	John Doe can reliably access secure work data.

Source: *FIPS PUB 199*

Types of FedRAMP Authorizations

The section below outlines the two types of FedRAMP Authorizations available to CSPs: a JAB Authorization and an Agency Authorization.

9.0 JAB Authorizations

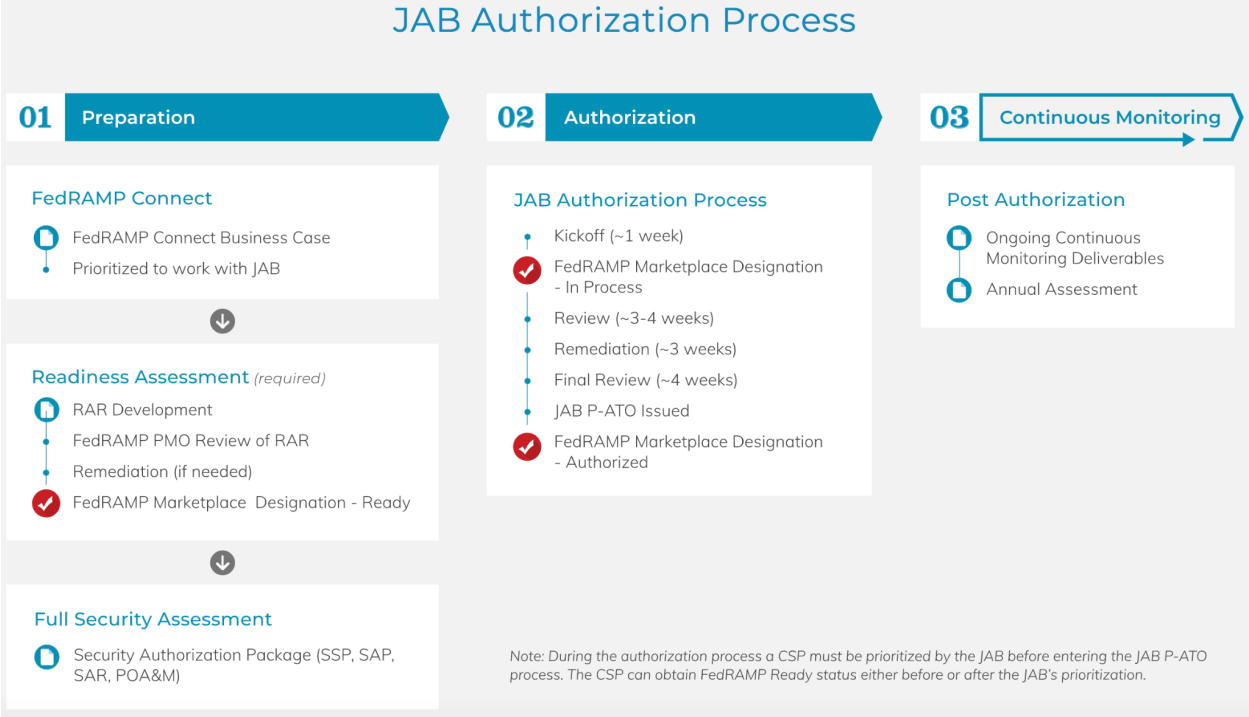

Figure 1: JAB Authorization Process Map

9.1. Phase 1: Preparation

FedRAMP Connect

The JAB invests heavily in creating a broad marketplace of providers and only has the capacity to authorize a limited number of CSOs a year based on current resources and funding. To ensure a clear return on investment of the resources used to authorize CSOs for the federal government, the FedRAMP PMO, CIO Council, and JAB evaluate CSOs via a process called FedRAMP Connect. During this process, CSOs develop business cases and are evaluated and prioritized to work with the JAB based on Prioritization Criteria.

The most important criteria for JAB prioritization is to demonstrate government-wide demand for the CSO. In order to ensure the FedRAMP PMO is evaluating each CSP's current and potential demand fairly, the CSP must provide proof of demand for their system from the equivalent of six (6) customers. There are multiple ways for a CSP to prove demand for their CSO; however, CSPs are not expected to meet all demand categories. The established demand categories ensure that the CSP's product will be broadly used by a

critical mass of government agencies. After achieving a JAB P-ATO, CSPs are expected to obtain a minimum of six (6) unique federal agency customers with authorizations that leverage the system's JAB P-ATO as part of their Continuous Monitoring requirements.

The JAB prioritizes up to 12 CSOs a year to work toward a JAB Authorization. After a CSP is prioritized, it has 60 days to become FedRAMP Ready (if it isn't already). Being prioritized to work with the JAB and being deemed FedRAMP Ready by the FedRAMP PMO constitute the first phase of the JAB Authorization process.

FedRAMP Ready

A FedRAMP Ready designation is required for any CSP pursuing a JAB P-ATO, and is highly recommended prior to pursuing an agency ATO. While becoming FedRAMP Ready is not a guarantee that a CSO will be authorized, CSOs who are FedRAMP Ready have preference in prioritization as the federal government has a clearer understanding of a CSP's technical capabilities and their likelihood of success in the authorization process. When planning for the FedRAMP Authorization process, CSPs should consider that the FedRAMP Ready designation is only valid for one calendar year after approval from the FedRAMP PMO.

In order to kick off with the JAB, CSPs must achieve the FedRAMP Ready designation for their CSO. To achieve the FedRAMP Ready designation, a CSP must work with a FedRAMP-recognized Third Party Assessment Organization (3PAO) to complete a Readiness Assessment of its service offering. The Readiness Assessment Report (RAR) documents the CSP's capability, and provides the JAB with a snapshot of a CSO's security posture.

At the conclusion of the assessment, the 3PAO may deliver a Readiness Assessment Report (RAR) to the PMO if the 3PAO can attest to the CSO's readiness for the authorization process. RARs are typically reviewed by the FedRAMP PMO within two business weeks after submission. If there are any issues identified by the PMO in the review, feedback is given to the CSP about what needs to be fixed in order for the CSP to be deemed FedRAMP Ready. Once the PMO approves a RAR, the CSO is listed as FedRAMP Ready on the FedRAMP Marketplace. In addition to being required to pursue a JAB P-ATO, being designated as FedRAMP Ready on the Marketplace provides valuable exposure to potential agency customers who are researching CSOs that meet their organizational requirements.

As a note, CSPs can and should use the RAR for a self-assessment in order to prepare for FedRAMP and a FedRAMP Ready assessment with a 3PAO. These assessments are also intended to help CSPs understand any gaps in their current architectures or capabilities prior to beginning a FedRAMP assessment. This information helps CSPs understand the level of effort necessary to secure their systems according to FedRAMP requirements.

More information regarding steps to achieve FedRAMP Ready can be found in the FedRAMP Marketplace Designations for Cloud Service Providers.

Full Security Assessment

After a CSO is prioritized to work with the JAB and is deemed FedRAMP Ready, the CSP finalizes the System Security Plan (SSP) for the service offering and engages a FedRAMP-recognized 3PAO. The 3PAO develops a Security Assessment Plan (SAP), conducts a full security assessment of the service offering, and produces a Security Assessment Report (SAR). The CSP facilitates and participates in the assessment activities in accordance with the SAP. Finally, the CSP develops a Plan of Action and Milestones (POA&M) to track and

manage system security risks identified in the SAR. The SSP, SAP, SAR, and POA&M must be completed using FedRAMP templates and submitted together. The JAB will not review the documents one by one. Instead, the full security package, along with the first Continuous Monitoring submission, will be considered in its entirety and must be submitted to the PMO at least 2 weeks prior to a Kickoff Meeting with the JAB. The FedRAMP PMO will then work with the CSP and FedRAMP-recognized 3PAO to conduct a completeness check, and coordinate the JAB Kickoff Meeting.

9.2. Phase 2: Authorization

The JAB Authorization Process uses an agile methodology with multiple stage gates and the "fail fast" principle. The first stage gate is the JAB Kickoff. During this step, the CSP, 3PAO, and FedRAMP collaboratively review the CSO's system architecture, security capabilities, and risk posture. Based on the outcome of the Kickoff Meeting, the JAB will issue a "go" or "no-go" decision to proceed with the authorization process. The Kickoff is typically a combination of briefings and informal Q&A. Following the kickoff, the JAB conducts an in-depth review of the security authorization package. The CSP and 3PAO are expected to support JAB Reviewers by addressing questions and comments in a timely manner and participating in regular meetings. Once the JAB's review is complete, the CSP and 3PAO remediate outstanding issues. Once completed, the JAB will issue a formal authorization decision and if favorable, issue a Provisional Authorization to Operate (P-ATO).

CSPs can be removed (a no-go decision) from the process for any number of reasons, although it is generally due to a major architectural issue or other deficiency that cannot be resolved during the authorization phase. The CSP and 3PAO representatives must be able to answer in-depth questions about the system architecture, risk management activities, actual risks to the system, and remediation planning/status.

If the Kickoff results in a go decision, the JAB conducts an in-depth review of the security authorization package. The CSP and 3PAO are expected to support JAB Reviewers by addressing questions and comments in a timely manner and participating in regular meetings with the 3PAO, FedRAMP PMO, and JAB Reviewers. During the review, the CSP must submit monthly ConMon deliverables (scan files, POA&M, and up-to-date inventory) which adhere to FedRAMP requirements for Continuous Monitoring and vulnerability scanning. The purpose of this requirement is to demonstrate maturity in the CSP's Continuous Monitoring capability. The first ConMon submission must coincide with the authorization package submission, two weeks prior to the kickoff meeting. The second ConMon submission must occur within 30 days of the first and establishes the CSP's normal monthly delivery date. Subsequent ConMon submissions must occur monthly throughout the authorization phase.

Once the JAB review is complete, the CSP and 3PAO remediate system and documentation issues as needed and ensure all JAB Reviewer comments are appropriately addressed. The CSP and 3PAO will then deliver their portions of the revised authorization package with all JAB Reviewer comments addressed. Once the JAB Reviewers have reviewed and validated the remediation efforts, the CSP will receive a P-ATO decision and formal provisional authorization of their CSO from the JAB.

The JAB P-ATO signifies that all three JAB agencies reviewed the security package and deemed it acceptable for the federal community. In turn, agencies review the JAB P-ATO and the associated security package and clear it for their agencies' use. In doing so, the agency issues their own authorization to use the product. A JAB P-ATO is not a risk acceptance but an assurance to agencies that the risk posture of the system has

been reviewed and approved by DoD, DHS, and GSA. Each agency must review and issue their own ATO which covers their agency's use of the cloud service. Information on a CSP's roles and responsibilities within the JAB P-ATO authorization process can be found here.

9.3. Phase 3: Continuous Monitoring

Following the issuance of a JAB P-ATO, the CSP is required to maintain a security posture that aligns with FedRAMP's requirements, pursuant to the initial assessment, and authorization process. This is achieved through Continuous Monitoring of the CSP's system. Described in NIST SP 800-137, the goal of Continuous Monitoring is to provide: (1) operational visibility, (2) managed change control, and (3) attendance to incident response duties over the life or use of a system. For more in-depth information about Continuous Monitoring requirements, please see the FedRAMP Continuous Monitoring Strategy Guide.

For systems with JAB P-ATOs, the JAB acts as a centralized PMO for Continuous Monitoring activities for those systems, providing agencies with the artifacts and a standard process for the assessment and management of JAB P-ATO systems. In this capacity, the JAB:

- Reviews and approves Continuous Monitoring and security artifacts on a regular basis
- Monitors, suspends, and revokes a system's P-ATO as appropriate
- Authorizes or denies Significant Change and deviation requests
- Reviews incident information to ensure proper handling and closure
- Ensures the FedRAMP PMO is providing artifacts to leveraging agencies in a timely manner

For leveraging agencies, the final approval authority for the use of a system is informed by the JAB's Continuous Monitoring artifacts and rests with each agency's designated AO.

In addition to the above described Continuous Monitoring activities, a CSP must utilize a FedRAMP-recognized 3PAO to complete an annual security assessment. Annual security assessments update a system's penetration testing results and perform comprehensive assessment of critical controls as well as a full assessment of all system controls over the course of three years.

10.0 Agency Authorization

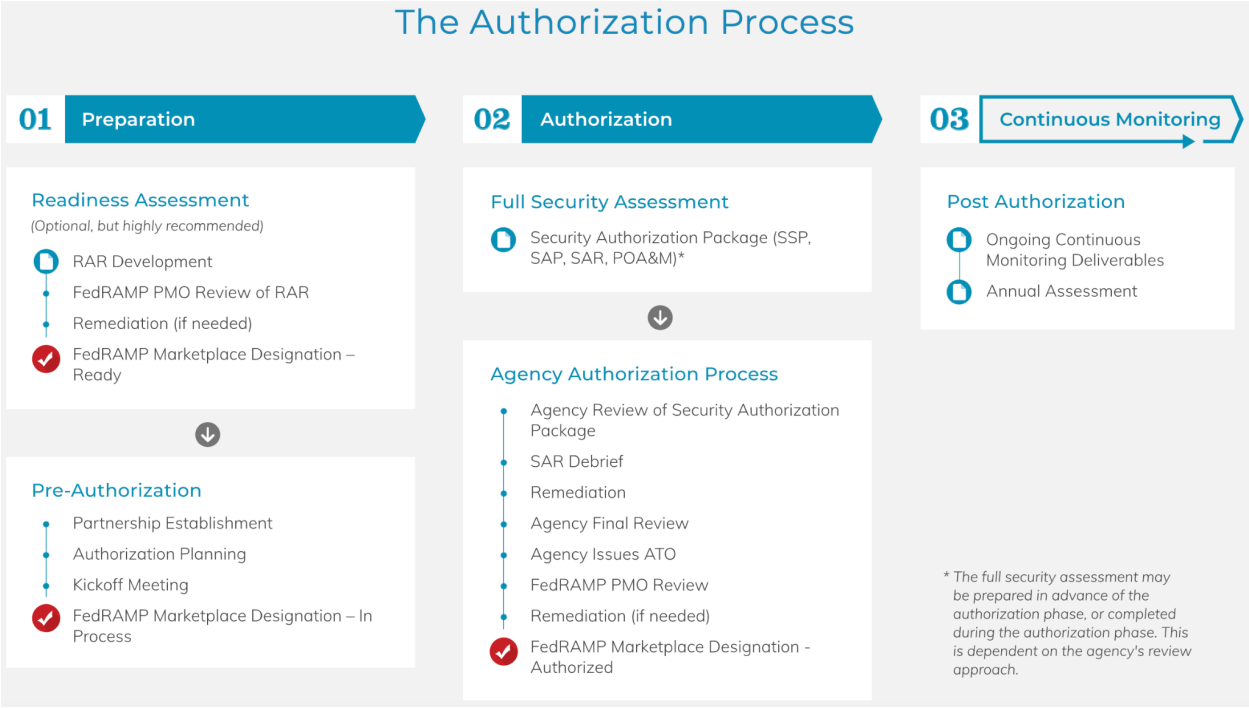

Figure 2: Agency Authorization Process

This is the same as the process displayed in our Agency Authorization Playbook, but it is from the CSP's perspective. It includes additional steps that both the CSP and agency would complete.

10.1. Phase 1: Preparation

FedRAMP Ready

A FedRAMP Ready designation is optional for the Agency Authorization process, but highly recommended. To achieve the FedRAMP Ready designation, a CSP must work with FedRAMP-recognized 3PAO to complete a Readiness Assessment of its service offering. The RAR documents the CSP's capability to meet federal security requirements.

CSP's that achieve the FedRAMP Ready designation are listed on FedRAMP's Marketplace. Agencies use the FedRAMP Marketplace to research cloud services that meet their organizational requirements. If a CSP is interested in pursuing government clients, becoming FedRAMP Ready makes available valuable information about the service offering's security for potential agency customers via the FedRAMP Marketplace.

Additionally, for CSPs who are considering whether or not to become FedRAMP Authorized, the RAR can serve as a self assessment to determine what gaps in their service offering's security exist and where those gaps might be. Such information can help CSPs understand the level of effort necessary to secure their system(s) according to FedRAMP requirements, prior to pursuing an ATO with an agency.

More information regarding steps to achieve FedRAMP Ready can be found in the FedRAMP Marketplace Designations for Cloud Service Providers.

Pre-Authorization

Partnership Establishment

In the partnership establishment phase of Pre-Authorization, a CSP formalizes their partnership with an agency meeting the requirements outlined in FedRAMP Marketplace Designations for Cloud Service Providers. In some cases, a vendor may be under contract with an agency already, or an agency may be working through the acquisition process. At this stage, a CSP should have a fully operational system and an executive team that is committed to the FedRAMP process. CSPs should engage with the FedRAMP PMO through the intake process by filling out a CSP Information Form. By completing this form, the PMO will also generate a FedRAMP ID for the CSO.

Prior to identifying an agency partner, a CSP should determine the security categorization of the data that will be placed within the system. CSPs should use the FedRAMP FIPS 199 Categorization Template (Attachment 10) in the SSP along with the guidance of NIST Special Publication 800-60 volume 2 Revision 1 to correctly categorize their system based on the types of information processed, stored, and transmitted on their systems. This analysis will inform a CSP as to which impact level is most appropriate for their system. Once a partnership is in place, a CSP should confirm their impact level with the agency, which will conduct its own FIPS 199 assessment.

Authorization Planning

Once the partnership is established, a CSP should:

- Confirm resources dedicated to the authorization process (which should include one technical writer, one technical SME, and one project manager at a minimum)
- Work with the agency to select a 3PAO for the assessment in Phase 2 (preferably with a FedRAMP-recognized 3PAO, though CSPs can utilize independent assessment organizations for agency ATOs)
- Complete FedRAMP training for CSPs
- 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.

- Complete a Work Breakdown Structure (WBS) with the assistance of your agency partner. After the completion of the WBS, please send this to the PMO for review.
- Work with your agency partner to complete an In-Process Request, the completion of this form indicates to the PMO that the CSP is able to begin scheduling a Kickoff Meeting.
- Begin working on the Kickoff Briefing Deck. A copy of your completed deck should be sent to the FedRAMP PMO prior to scheduling the Kickoff Meeting.
    - The PMO has a guidance document that CSPs can use when developing their presentation. This will be shared with CSPs at the conclusion of an intake call. If you have not had an intake call, please reach out to info@fedramp.gov for a copy of the guidance.

Kickoff Meeting

The final step in this phase is to prepare for and conduct a 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 making sure everyone is aligned on the overall process and milestone timelines. Though the FedRAMP PMO coordinates and facilitates Kickoff Meetings, kickoffs are ultimately meant to be in service of the CSP and agency partnership.

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 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

At the conclusion of this meeting, CSPs are able to gain access to FedRAMP's secure repository (unless the system's impact level is High). Additionally, CSPs that are not already listed as In Process on the FedRAMP Marketplace are eligible to be listed if the agency is comfortable with the briefing and timelines. Please note that not all systems will be eligible to be listed based on the Kickoff Meeting, so be sure to engage with the PMO on your In Process status after this step.

> **IN-PROCESS DESIGNATION**
>
> CSPs are considered FedRAMP In Process once they are actively working toward a FedRAMP Authorization, either through the JAB or in an established partnership with an agency. The FedRAMP Marketplace Designations for Cloud Service Providers outlines the requirements for achieving this designation. Once In Process, CSPs are displayed on the FedRAMP Marketplace with this designation.

> While your agency point of contact (POC) may be someone on the program side, it is critical to connect with the security side of the agency and, ultimately, its Authorizing Official, who is required to send an In Process Request to FedRAMP prior to a CSP achieving an In Process designation. If your program owner does not know who to go to in their agency for this, the PMO can assist.

10.2. Phase 2: Authorization

Full Security Assessment

During this phase, the 3PAO tests the CSP's system. The SSP should be fully developed and the CSP should engage with their 3PAO to develop a SAP. If the CSP has partnered with an agency using the Just-In-Time linear approach described in the table above, it is recommended the agency approve the SAP before the 3PAO initiates testing. During testing, it is critical that no changes are made to the system, and that it is frozen from a development perspective. Once the testing is complete, the 3PAO will develop a SAR, which details their findings and includes a recommendation for FedRAMP Authorization. The CSP will then develop a POA&M based on the SAR findings and include input from the 3PAO, which outlines a plan for addressing the findings from testing.

Once this has been completed, the CSP and 3PAO should work to complete a SAR Debrief presentation. Please send a completed copy of this deck to the PMO for review prior to scheduling the SAR Debrief meeting. The PMO has a guidance document that will be shared at the conclusion of the Kickoff Meeting.

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. Though the PMO coordinates and facilitates the SAR Debrief, it is ultimately 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 (e.g.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

Agency Authorization Process

Once the assessment and associated deliverables are complete, the agency reviews them and either approves them or requests that additional testing take place. A final review is then conducted, and if the agency accepts the risk associated with the use of the system, they provide an Authorization to Operate (ATO) letter signed by the Authorizing Official.

After the agency AO issues their 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 broad brush 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'

Once the ATO letter is received by the PMO, 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 • OMB MAX for Low and Moderate baseline packages • CSP's repository for High baseline 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 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 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

Once a CSO receives a FedRAMP Authorized designation, the FedRAMP Marketplace will be updated to reflect the designation. The FedRAMP PMO will make the CSO security package available, upon request and validation of the requestor, to the entire federal government for the purpose of issuing subsequent ATOs for the use of the service based on their own reviews of the CSO's security documentation. Due to the sensitivity of the materials, this information is highly controlled through the use of the FedRAMP Package Access Request Form that must be routed through appropriate signatures within the federal government. Each form requires the FedRAMP PMO's approval to review the documents.

> Once a cloud service has achieved a FedRAMP Authorized designation, each subsequent agency customer must still provide their own ATO for the use of the service. Agencies have an easy path to this view of FedRAMP's reuse model; once the authorization is complete, any agency may review the security package, determine acceptability of risks associated with using the service, and issue their own ATO. If any agency customers are confused about this process, the FedRAMP PMO can support calls to discuss it. All ATO letters should be sent to the FedRAMP PMO for monitoring.
>
> FedRAMP's Quick Guide for Reusing Authorizations for Cloud Products outlines the step-by-step process for agencies to issue their own ATOs for FedRAMP Authorized CSOs.

10.3. Phase 3: Continuous Monitoring

Once the FedRAMP Authorization is complete, a CSP must provide monthly Continuous Monitoring deliverables to the agencies that are using their service. These deliverables include an updated POA&M, vulnerability scan results/reports, deviation requests, Significant Change requests, incident reporting, and the Annual Assessment package. Each agency using the service reviews the monthly Continuous Monitoring deliverables. CSPs with cloud offerings categorized at LI-SaaS, Low, or Moderate use the FedRAMP secure repository for posting monthly Continuous Monitoring materials. CSPs with cloud offerings categorized at High use their own secure repository.

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. If you are a FedRAMP Authorized CSO and would like to engage the PMO to help set up a Multi-Agency ConMon Group, please reach out to info@fedramp.gov to request assistance.

Additionally, a CSP must employ a 3PAO to complete an annual security assessment to ensure that the risk posture of the system is maintained at an acceptable level throughout the lifecycle of the system. The Annual Assessment, along with updated security authorization package documentation, must be uploaded to the FedRAMP secure repository, and FedRAMP should be notified via info@fedramp.gov when this is complete.

Important Considerations

Below are some areas of consideration as you develop your authorization strategy. We recommend you understand these areas and be prepared to talk about them during your intake call with the FedRAMP PMO.

11.0 IaaS vs. PaaS vs. SaaS

NIST SP 800-145 establishes FedRAMP's definitions for cloud services that are IaaS, PaaS, or SaaS. CSPs needing to define their offerings as one or multiple of the service models should refer to the following guidelines:

	Definition
Software-as-a-Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Platform-as-a-Service (PaaS)	The capability provided to the consumer is to deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Infrastructure-as-a-Service (IaaS)	The capability provided to the consumer is to provide processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

12.0 System Stack

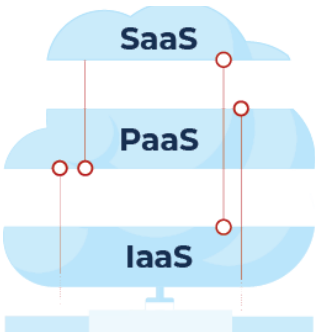

Figure 4. System Stack

The "system stack" generally refers to the layers of services in the data center that are included in the Cloud Service Offering. The CSO must be authorized according to the appropriate FedRAMP baseline, meaning each component (IaaS, PaaS, SaaS) must be authorized.

Using a SaaS CSO as an example, an authorized stack would include three system boundaries and ATO letters for each component layer. This lends the

SaaS the ability to inherit/leverage security controls from the underlying PaaS/IaaS layers, transferring responsibility for the maintenance of some controls to the CSP providing infrastructure services.

When a CSP has its system hosted in a non-FedRAMP Authorized cloud service, the "inheritance/leveraging" relationship does not exist. In this situation, a SaaS provider would need to include the infrastructure and platform within its authorization boundary, in addition to its own software application, to authorize the entire stack. The CSP is responsible for the entire stack in this situation and details the underlying infrastructure and platform within its SSP. The authorization in this case, would be for the SaaS with its own infrastructure, but the infrastructure itself would not constitute an IaaS.

The FedRAMP PMO highly recommends that CSPs understand a system's stack and to illustrate how IaaS, PaaS, and SaaS may be layered. Additionally, the PMO can inform CSPs on how existing ATOs can be leveraged depending on the system architecture.

> **NOTE:** *To achieve a JAB Authorization, the CSP's service must reside on a JAB Authorized infrastructure (list of JAB Authorized infrastructures) or stand up their own infrastructure.*

13.0 Level of Effort

The level of effort (LOE) and cost associated with authorizing a CSO will vary depending on the complexity of the system and overall commitment and expertise of the team. Additionally, overall LOE and cost will depend on whether a CSP pursues an agency ATO or a JAB P-ATO, as each agency follows a slightly different authorization process contingent on their agency's specific security requirements.

LOE can be broken down into the following categories:

	Definition
Project Management	Making changes to the system in compliance with agency and FedRAMP controls
Documentation	Completion of all required documentation, including technical writing, review, and quality assurance of documentation submitted to agencies, JAB, and FedRAMP PMO
Support	Costs associated with consultants and advisory services acquired to support the authorization, including appropriate technical expertise and assessment services provided by a 3PAO

Typical barriers for CSPs completing the authorization process that will impact overall LOE include:

- Not accurately defining the authorization boundary or depicting data flow diagram(s)
- Not having FIPS 140 validated encryption modules
- Not implementing multi-factor authentication appropriately
- Poor documentation and immature management processes
- Not applying appropriate resources up front (e.g. failing to bake security and resources in early)

13.1. CSP Authorization Team

Staffing an authorization effort, either JAB or Agency Authorization, should be a key consideration for any CSP. While the FedRAMP PMO does not recommend any specific resource leveling, it has witnessed successful authorization efforts when the following competencies are included on a CSP authorization team, either in an in-house or consulting capacity:

	Definition
Project Management	Experience with team and task management as part of information technology (IT) system implementation with federal or large-scale private organizations, including prior FedRAMP or FISMA authorization experience. Successful project managers typically have a working knowledge of Agile, DevOps, or Lean management approaches. Additionally, they are comfortable in the coordination of project stakeholders and have end-to-end visibility of the implementation of an IT system.
Customer Relationship Management	Typically, a sales or business development associate familiar with or responsible for the business relationship leading to the federal procurement of a system. Successful customer relationship managers facilitate communications among stakeholders throughout the implementation effort, especially during the initial partnership of CSP and agency resources at the beginning of an authorization effort.
System Architecture and Engineering	Informed expertise regarding the service offering's system architecture and design, including visibility to the adaptation of applicable security controls to the system. Effective technical personnel in an authorization effort often demonstrate competency with federal IT systems and a thorough understanding of federal security requirements as defined by FISMA and FedRAMP.
Technical Writing	Effective writing capability that is informed by a thorough understanding of a system's architecture and design and how applicable security controls affect and interact with the system. Additionally, effective technical writers demonstrate a working knowledge of how controls relate to the service offering, the agency, and any underlying systems within the system stack (e.g., IaaS inheritance).
Communications	The FedRAMP PMO considers communications to be a core competency of any project team and can be reflected in a dedicated full-time equivalent (FTE) or represented in the aggregate skill sets of the CSP team. Communications are integral to the ongoing coordination of CSP, agency, 3PAO, and PMO resources throughout the lifecycle of a system in a federal environment.

VOLUME II:

DEVELOPING AN AUTHORIZATION PACKAGE

Introduction

CSP Playbook Volume II: Developing an Authorization Package is the second volume in FedRAMP's CSP Playbook series. *Volume I* described how Cloud Service Providers (CSPs) can get started with FedRAMP, introducing the Agency and Joint Authorization Board (JAB) Authorization processes, FedRAMP designations, and what CSPs should consider prior to pursuing an authorization.

Volume II provides an overview of the elements of an authorization package, along with general guidance and tips for delivering a high-quality package that will ensure an expeditious authorization process. The overall goal of Volume II is to minimize rework and delays by helping CSPs get it right the first time. We will continue to update this volume as we identify additional guidance and tips for success.

This volume applies to CSPs pursuing a FedRAMP Authorization at the Low, Moderate, or High impact levels and is intended to supplement the information provided in the on-demand CSP Training. In addition to reviewing this document in its entirety, CSPs pursuing a FedRAMP Authorization must also take the on-demand training.

What's in an Authorization Package

A FedRAMP authorization package documents the security and risk posture for a CSP's Cloud Service Offering (CSO). It includes the System Security Plan (SSP), which is the "security blueprint" for the CSO. The SSP defines the CSO's authorization boundary and describes the security controls in place to protect the confidentiality, integrity, and availability (CIA) of the system and federal data. The authorization package also includes several required SSP attachments (e.g., Policies and Procedures and Incident Response Plan), Security Assessment Plan (SAP), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), and authorization letter.

FedRAMP authorization packages are leveraged by federal agencies for the authorization of cloud services for federal government use. FedRAMP provides standard templates and resources for CSPs to develop and deliver authorization packages to federal customers.

- System Security Plan (SSP) and attachments
- Security Assessment Plan (SAP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POA&M)
- Signed agency Authorization to Operate (ATO) - For Agency Authorizations
- Signed JAB Provisional-ATO (P-ATO) - For JAB Authorizations

Table 1. FedRAMP Authorization Package: Inventory of Documents

FedRAMP Authorization package documents must be submitted in designated formats (e.g., MS Word, MS Excel), and some must be prepared using a FedRAMP-provided template. CSPs are required to complete and submit the FedRAMP Initial Authorization Package Checklist to ensure that all documentation requirements are met. The Checklist indicates required submission formats and templates, and must be included with the initial authorization package.

CSPs and 3PAOs are prohibited from altering or removing content in the SSP, SAP, and SAR templates. However, CSPs and 3PAOs should remove the blue italicized instructional text before submitting the final versions of the SSP, SAP, and SAR. agency-specific requirements, above and beyond the FedRAMP baseline, must be documented in an appendix to the SSP.

Developing an Authorization Package

The following sections describe the roles and responsibilities with respect to the development of the authorization package, as well as general guidance for completing the SSP, SAP, SAR, and POA&M.

FedRAMP encourages stakeholders to review the program's automation initiatives that aim to reduce the level of effort to prepare authorization materials. The Open Security Controls Assessment Language (OSCAL), developed in partnership with NIST, enables CSPs to prepare security authorization documents in a machine-readable format. To gain an understanding of the purpose and benefits of using OSCAL, the program encourages CSPs to review the program website and associated guidebooks.

1.0 Roles and Responsibilities

CSPs and 3PAOs should understand and agree on the division of roles and responsibilities with respect to the development of an authorization package. Although CSPs do not develop the SAP and SAR, they are responsible for reviewing and approving these documents. For this reason, this CSP Playbook Volume II includes several tips on how to review the SAP and SAR for completeness, correctness, and consistency.

	CSP	3PAO
SSP	• Develop SSP documentation using FedRAMP templates* • Validate work prepared by advisors (if applicable)	• As an advisor, develop the SSP documentation** • As an assessor, validate SSP documentation is complete and accurate**
SAP	• Review and approve SAP • Sign Penetration Test Rules of Engagement	• Coordinate with CSP to define assessment scope and methodology • Deliver SAP and Security Test Case Procedures using FedRAMP templates***

		• Sign Penetration Test Rules of Engagement • Deliver Penetration Test Plan that aligns with FedRAMP's guidance
SAR	• Provide required artifacts and evidence to 3PAO during assessment • Work with 3PAO to identify risks that must be remediated or mitigated prior to authorization	• Perform assessment of CSO according to FedRAMP guidelines • Draft a SAR that aligns with SSP/SAP detail and describes the findings of the assessment*** • Deliver the SAR to the CSP
POA&M	• Create and maintain a POA&M that aligns with FedRAMP's POA&M Template and Completion Guide • Implement monthly Continuous Monitoring • Use the POA&M to track and manage risks	• Validate POA&M detail for a CSO as part of annual assessment • If performing POA&M activities on behalf of a CSP, assume all CSP responsibilities for POA&M management

Table 2. CSP and 3PAO Roles and Responsibilities for Authorization Packages

** CSPs are required to use FedRAMP templates for the SSP, Privacy Impact Assessment (PIA), Rules of Behavior (RoB), Information System Contingency Plan (ISCP), Control Implementation Summary (CIS) Workbook, Laws and Regulations, Integrated Inventory Workbook, and Plan of Action and Milestones (POA&M). CSPs develop their own Policies and Procedures, User Guides, Incident Response Plans and Configuration Management Plans. Additional guidance on each of these required documents is provided in the sections below.*

*** Per R311: Specific Requirements - FedRAMP, 3PAOs contracted to provide advisory services cannot provide assessment services for the same CSO for a period of two years.*

**** 3PAOs are required to use FedRAMP templates for the SAP, Security Test Case Procedures, SAR, and Risk Exposure Table.*

2.0 System Security Plan (SSP)

A SSP is the "security blueprint" for the Cloud Service Offering. A well-written SSP allows the reviewer to pull the thread between the system's architecture, data flows, security control implementations, and authorization boundary. After reviewing the SSP, the AO (or designee) should have a strong understanding of how federal data is transmitted to, from, and within the system; where the data is processed and stored; and how the data is protected.

FedRAMP provides an SSP template for each of its baselines: Low, Moderate, and High.

When drafting the SSP, keep in mind that it is telling a story about the security of your Cloud Service Offering. If there are gaps in the storyline, you will be required to address the gaps, which can delay the authorization process.

2.1. Getting Started: Focus on Quality

A high-quality SSP is the key to success. If you do not have a strong technical writer with security experience on your team, hire one! Though it is not required, CSPs often choose to hire an experienced advisory partner to help develop the SSP. Many of the approved 3PAOs listed on the FedRAMP Marketplace provide advisory services in addition to assessment services.

NOTE: If engaging a 3PAO advisor, a different 3PAO must be engaged to perform the independent assessment.

A common barrier to success is a poorly written, incomplete, inaccurate, and/or inconsistent SSP. FedRAMP has defined general criteria for document acceptance in **Table 3** below. In addition, before beginning the process of documenting the SSP, CSPs should complete the following FedRAMP Online Training modules: FedRAMP System Security Plan (SSP) Required Documents (200-A) and How to Write a Control (201-B). We also provide further guidance and expectations associated with effective control writing later in this section.

Table 3. Criteria for Document Acceptance

Criteria	Description
Clarity	• Logical presentation of material • Current dates and timely content • Non-standard terms, phrases, acronyms, and abbreviations defined • No ambiguous statements or content • Correct grammar and free from awkward phrases, typographical errors, spelling errors, missing words, or incorrect page and section numbers • Readable figure text • Sharp and legible figure graphics
Completeness	• Includes accurate, detailed, and informative content that is consistent with FedRAMP requirements • Includes all appropriate sections of FedRAMP templates • Includes all attachments and appendices • Includes Tables of Contents, List of Tables, and List of Figures where applicable • Includes figures with required information, correct labels, and keys to color and line formats
Conciseness	• Content and complexity relevant to the audience • No superfluous words or phrases

Consistency	• Correct and consistent format • Correct and continuous section numbering • Terms with the same meaning throughout the document • Items that are referred to by the same name or description throughout the document • Level of detail and presentation style that are the same throughout the document • Material that does not contradict predecessor documents • All material in subsequent documents based in the predecessor document • Figure content that agrees with text

2.2. Getting Started: Define the Authorization Boundary and Data Flows

Before implementing and documenting security controls, CSPs must clearly define the authorization boundary for the CSO. The authorization boundary provides the reviewer with a clear understanding of what exactly is being authorized, and is the foundation on which the remainder of a SSP is built. The authorization boundary is validated against the inventory during the 3PAO assessment.

The Authorization Boundary Diagram (ABD) is a visual representation of the system services, components, and devices that make up the authorization boundary for the CSO. To help Authorizing Officials (AOs) understand areas that may require risk-acceptance or areas where the agency has responsibility (that is, everything excluded from the authorization boundary), the ABD also depicts all *external* systems or services that provide functionality to the CSO or are used to manage and operate the CSO. This includes underlying IaaS/PaaS offerings, system interconnections, APIs, external cloud services, corporate-shared services, and update services (e.g., malware signatures and OS updates).

To properly define the authorization boundary, CSPs need to understand how and where federal data and metadata flow through and within the CSO. To that end, CSPs should begin by depicting data flows internal and external to the CSO.

To understand how to define the authorization boundary, CSPs must review the FedRAMP Authorization Boundary Guidance.

2.3. Moving on: Writing the SSP

Once the authorization boundary and data flows are defined, CSPs can begin to implement security controls and write the SSP.

Sections 1 through 12 of the SSP are referred to as the “front matter”. These sections include general information about the CSO (e.g., FIPS 199 categorization, service model, deployment model) as well as detailed descriptions of the CSO’s function, system architecture, authorization boundary, data flows, interconnections, and so on. This section provides guidance on how to properly document security controls in the SSP.

Each and every control in the FedRAMP SSP template contains three sections: Control Requirement(s), Control Summary Information, and Control Implementation Statement. Guidance related to each section is provided below, along with a list of “Dos and Don’ts” to ensure success.

2.3.1. Control Requirement

FedRAMP's baselines are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 catalog of security and privacy controls for federal information systems. Security controls may include a single requirement or may be broken down into several requirements.

A requirement that begins with "The information system…" generally refers to a technical capability that must be in place. For example, IA-2(1) requires the information system to *implement multifactor authentication for network access to privileged accounts.*

A requirement that begins with "The organization…" generally refers to a process or procedure that must be in place. For example, IR-5 requires the organization to *track and document information system security incidents*.

Many control requirements include *parameters* that are defined by the CSP or defined by FedRAMP. Some controls also include additional FedRAMP Requirements and/or Guidance. Let's use IA-4 as an example:

IA-4 Identifier Management

The organization manages information system identifiers for users and devices by:

(a) Receiving authorization from [*Assignment: organization-defined personnel or roles*] to assign an individual, group, role, or device identifier;

Hint: The organization (CSP) defines which person or role can authorize the assignment of identifiers

(b) Selecting an identifier that identifies an individual, group, role, or device;
(c) Assigning the identifier to the intended individual, group, role, or device;
(d) Preventing reuse of identifiers for [*FedRAMP Assignment: at least two (2) years*]; and

Hint: CSPs cannot define this parameter. FedRAMP requires CSPs to prevent the reuse of identifiers for at least 2 years

(e) Disabling the identifier after [*FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)*]

Hint: CSPs cannot define this parameter for user identifiers. FedRAMP requires user identifiers to be disabled after 90 days of inactivity. CSPs can define this parameter for device identifiers as indicated by the additional FedRAMP requirement below.

IA-4e Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD (Department of Defense) clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP.

2.3.2. Control Summary Information

The FedRAMP SSP template includes a Control Summary Information table for each control. This table includes the following fields which must be completed by the CSP. The information in this table must be consistent with the control implementation statement (i.e., the control narrative) and the Control Implementation Summary (CIS) Workbook. We will discuss the CIS in the next section: SSP Attachments.

- Responsible Role: The role (e.g., Database Administrator, Account Manager, ISSO) that can best respond to questions about the particular control. It is typically the role responsible for implementing, managing, and monitoring the control. Actual names of individuals should NOT be provided.
- Parameter(s): Enter the actual parameter value in the appropriate field. In the IA-4 example above, the Control Summary Information table would include three parameter fields for IA-4(a), IA-4(d), and IA-4(e).
- Implementation Status: At least one status must be selected for each control.
    - For controls with multiple requirements, a CSP may need to select more than one status. For example, AC-8 requires the system to:
        - (a) display a system use notification message before granting access to the system AND
        - (b) retain the message on screen until the user acknowledges the usage conditions by taking an explicit action
    - If the CSP has successfully implemented (a) but is still figuring out a way to implement (b), the CSP would select both "Implemented" and "Planned".

> If any portion of a control is "Planned" or "Partially Implemented," the control will be identified as "Other than Satisfied" during the 3PAO security assessment.

- Control Origination: All controls originate from a system or from a business process. It is important to correctly describe the control origination so that it is clear who is responsible for implementing, managing, and monitoring the control. Definitions and examples for each Control Origination can be found in Table 13-2 of the SSP, *Control Origination and Definitions*.
    - If the system is inheriting a control from a FedRAMP-Authorized IaaS/PaaS, select the "inherited" box and provide the name and/or FedRAMP ID of the underlying IaaS/PaaS along with the date of authorization. Controls can only be inherited from a pre-existing FedRAMP Authorization. If the CSO is hosted in an IaaS/PaaS not authorized by FedRAMP, there is no leveraging/inheritance relationship. In this scenario, the CSP is responsible for the entire stack, and the underlying components must be defined as part of the CSO's authorization boundary as system interconnections and external services.

> SSP authors should clearly indicate which portions of the security control are inherited and provide a description of *what* is inherited. Authors do not need to describe *how* the leveraged system implemented the control. That detail is found in the SSP of the leveraged system from which the control is inherited.

2.3.2. Control Implementation Statement: What is the Solution and How is it Implemented?

The Control Implementation Statement is the written narrative that describes what is implemented, how it's implemented, and who's responsible for it. Carefully read the control requirement(s) and ask yourself the following:

- Does the Control Implementation Statement address each and every requirement defined in the control? For multi-part controls, the implementation statement should only address the requirements associated with that part.
    - Every control part (Part a, Part b, Part c, etc.) should contain a focused discussion on the specific control requirement. Using the previous IA-4 example, the Part d narrative should describe the *measures in place to prevent the reuse of identifiers within the appropriate timeframe* and nothing more. Focusing the narrative on the specific requirement(s) will help expedite the review process.
- Is the implementation statement clear with no room for interpretation or confusion?
- Does the implementation statement explicitly state whether or not the control requirement is satisfied?
- Does the implementation statement clearly describe how the control is implemented, including who (what role) is responsible for implementing and/or enforcing the control?

NOTE: In some cases, describing the *how* is difficult because the answer may be complex or lengthy. In these cases, it is acceptable to describe the *how* at a high level and then point the reviewer to an external document for more detailed information.

Although reviewers will have varying degrees of technical and security expertise, they will not have a deep understanding of your CSO. Therefore, remove all ambiguity and guesswork by explaining all system-specific terms, components, etc.

TIP: Pay attention to the verbs in each of the control requirements. For example, IR-5 requires the CSP to track and document security incidents. In the control implementation statement for IR-5, CSPs must describe the process/tools employed to track incidents, as well as the process/tools employed to document incidents. To ensure that all control requirements are implemented and adequately addressed in the implementation statement, CSPs are encouraged to review the assessment objectives defined for each control in the FedRAMP Security Test Case Procedures template. Templates for the Low, Moderate, and High baselines are available on the Document & Templates page of the FedRAMP website.

TIP: For customer-provided, customer-configured, or shared controls, create a “Customer Responsibility” heading in the control implementation statement. Clearly describe what the customer is expected to do under this heading. You do not have to describe how the customer implements the requirement.

2.4. SSP Controls Do's and Don'ts

Do's	Don'ts

• **Do** ensure that all roles are defined in Table 9-1, *Personnel Roles and Privileges*, and are described consistently throughout the SSP.
• **Do** complete all fields in the Control Summary Information table and ensure the information is consistent with the control implementation statement.
• **Do** provide a rationale for Not Applicable (N/A) controls.
  ○ Many CSPs mistakenly identify controls as N/A if the capability is not authorized for use. For example, many CSPs consider AC-2(2) to be N/A because temporary/emergency accounts are not used in the environment. FedRAMP considers this control to be applicable and requires the CSPs to reference the policy that prohibits the creation of temporary/emergency accounts and describe any technical controls in place to prevent the creation of and/or audit unauthorized accounts.
• **Do** include correct and consistent document titles when referencing SSP attachments or other external documents.
  ○ If the entire referenced document does not apply, specific section references should be provided so the applicable sections can be located easily.
  ○ Provide the filenames of all SSP Attachments in Table 15-1 of the SSP, *Names of Provided Attachments*. This way, you only have to update the filename in one location.
  ○ For SSP Attachments 1-13, use the recommended file naming convention of <information system abbreviation> <attachment number> <document abbreviation> <version number>. For example, "Information System Abbreviation A8 IRP v1.0."
  ○ If referencing other external documents, use a standard naming convention, add the document name and filename to Table 15-1 of the SSP, and upload the documents to OMB MAX with the SSP package. NOTE: If an external document contains sensitive system information and cannot be uploaded to OMB MAX, include a statement in Table 15-1 to the effect of "this document contains sensitive system information, but can be provided upon request for audits and assessments."
	• **Don't** modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements/guidance. CSP responses must be documented in the "Control Summary Information" and "What is the solution and how is it implemented?" tables.
	• **Don't** simply repeat or rephrase the control requirement when writing the control implementation statement.
	• **Don't** reference other controls instead of providing a written control narrative. Referencing related controls for *additional detail* is acceptable, but each control needs to stand on its own with a narrative that adequately addresses the control requirement(s).
	• **Don't** reference SSP attachments or external documents instead of providing a written control narrative. Referencing SSP attachments or external documents as *examples* or for *additional detail* is acceptable as long as the control narrative adequately addresses the control requirement(s).
	• **Don't** copy and paste implementation statements from one control to another. The implementation statement should address the specific control requirement(s). It should not contain content that is not directly relevant to the control requirement.

2.5. SSP Attachments

Table 4 summarizes the required security attachments for a complete SSP. CSPs should understand the information required to complete each document and, where applicable, align and update existing organizational policy and processes to meet requirements outlined in the SSP attachments (e.g., Incident Response Plan, Configuration Management Plan, etc.).

Table 4. System Security Plan (SSP) Attachments

- Attachment 1: Information Security Policies and Procedures
- Attachment 2: User Guide
- Attachment 3: Digital Identity Worksheet*
- Attachment 4: Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)*
- Attachment 5: Rules of Behavior (RoB)*
- Attachment 6: Information System Contingency Plan (ISCP)*
- Attachment 7: Configuration Management Plan (CMP)
- Attachment 8: Incident Response Plan (IRP)
- Attachment 9: Control Implementation Summary (CIS)*
- Attachment 10: Federal Information Processing Standard (FIPS) 199 Categorization*
- Attachment 11: Separation of Duties Matrix
- Attachment 12: FedRAMP Laws and Regulations*
- Attachment 13: FedRAMP Integrated Inventory Workbook*

** Document must be submitted in FedRAMP templates.*

2.5.1. Attachment 1: Information Security Policies and Procedures

Policies and Procedures (P&Ps) are a critical supplement to the SSP and are required by the first control (known as the "dash ones", e.g., AC-1) for each control family. Policies provide the guidelines under which the procedures are developed and by which the SSP controls are implemented. Procedures define the specific instructions necessary to perform a technical task or business process. Procedures detail who performs the tasks, what steps are performed, when the steps are performed, and how the procedure is verified. Examples of procedures are:

- How to Create Accounts
- How to Test Backups
- Media Sanitization Procedures
- How to Review Logs for Suspicious Activity

FedRAMP does not provide templates for P&Ps. Some CSPs choose to combine all policies into a single document and all procedures into a single document. Some CSPs choose to develop separate P&Ps for each control family. Either approach is acceptable, as long as the requirements for each "dash one" control are satisfied, and the reviewer understands how to locate the P&Ps associated with each control family.

> **NOTE:** In some cases, a required FedRAMP SSP attachment may include procedures for a particular set of security controls. For example, the Information System Contingency Plan (ISCP) is a required SSP attachment. This plan establishes general procedures for recovering the CSO after a service disruption.

2.5.2. Attachment 2: User Guide

The User Guide explains how agency customers will use the system. For example, if the system has a self-service portal, the User Guide must explain how to use the portal.

FedRAMP does not provide a template for the User Guide. Many CSPs provide guidance and instructions to agency customers via a dynamic website versus a separate static document. This is perfectly acceptable. Be sure to note the website address in Table 15-1 of the SSP. If the information is not publicly accessible, include instructions for requesting access.

2.5.3. Attachment 3: Digital Identity Worksheet

CSPs are required to complete the Digital Identity Worksheet, embedded as Attachment 3 in Section 15 of the FedRAMP SSP Template (a separate attachment is not required). The Digital Identity Worksheet provides guidance on selecting the appropriate level for the following components of identity assurance:

- Identity proofing process (IAL)
- Authentication process (AAL)
- Assertion protocol used in a federated environment to communicate authentication and attribute information (FAL)

Table 15-3 of the SSP, *Mapping FedRAMP Levels to NIST SP 800-63-3 Levels*, maps the FedRAMP impact levels (Low, Moderate, and High) to NIST SP 800-63-3 levels (1, 2, and 3).

2.5.4. Attachment 4: Privacy Threshold Analysis/Privacy Impact Assessment (PTA/PIA)

All authorization packages must include a PTA and, if necessary, a PIA. The PTA template is embedded as Attachment 4 in Section 15 of the FedRAMP SSP Template (a separate attachment is not required). The PTA includes four qualifying questions to determine if Personally Identifiable Information (PII) is collected by any component of the CSO. If the answer to any of the qualifying questions is "Yes", the CSP must complete the FedRAMP PIA Template and submit it as an attachment to the SSP.

> **NOTE:** Federal cloud customers (data owner/system owners) are required to perform their own PIAs and may share this information with the CSP if they so desire for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII.

2.5.5. Attachment 5: Rules of Behavior (ROB)

Security control PL-4 requires CSPs to develop Rules of Behavior (RoB) that establish and describe the responsibilities and expected behavior related to the use of the CSO.

FedRAMP provides a RoB Template that includes two example sets of Rules of Behavior: one for internal users and one for external users. CSPs should tailor these rule sets as appropriate to define the rules of behavior necessary to secure the CSO.

2.5.6. Attachment 6: Information System Contingency Plan (ISCP)

Security control CP-2 requires CSPs to develop a Contingency Plan for the CSO. FedRAMP provides an ISCP Template that CSPs must use to establish comprehensive procedures to recover the CSO quickly and effectively following a service disruption.

NOTE: Keystroke-level procedures are not commonly included in the ISCP. These procedures are typically considered system sensitive and are only shared when required for audits and assessments.

TIP: A Business Impact Analysis (BIA) is required as Appendix M of the ISCP. FedRAMP does not provide a BIA template; however, NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, includes a sample BIA template in Appendix B.

NOTE: Security control CP-4 requires CSPs to test the ISCP at least annually and document the results in a test report. The test report must be included in the ISCP. Some CSPs incorrectly assume that this requirement only applies during ongoing Continuous Monitoring (post-authorization). CSPs must conduct a test of the ISCP prior to achieving a FedRAMP Authorization and at least annually thereafter as part of Continuous Monitoring.

2.5.7. Attachment 7: Configuration Management Plan (CMP)

Security control CM-9 requires CSPs to develop a Configuration Management Plan (CMP). FedRAMP does not provide a template for the CMP. However, NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, provides guidelines for the implementation of CM controls as well as a sample CMP outline in Appendix D of the Guide.

2.5.8. Attachment 8: Incident Response Plan (IRP)

Security control IR-8 requires CSPs to develop an Incident Response Plan (IRP). FedRAMP does not provide an IRP template; however, NIST SP 800-61, *Computer Security Incident Handling Guide*, provides guidance on the development of incident response policies and procedures as well as guidance on the development of an Incident Response Plan.

TIP: When developing the IRP, be sure to incorporate the incident reporting requirements defined in the FedRAMP Incident Communications Procedures. This document outlines the steps for FedRAMP stakeholders to use when reporting information concerning information security incidents, including response to published Emergency Directives.

NOTE: Security control IR-3 requires CSPs to test the IRP at least annually and document the results. Some CSPs incorrectly assume that this requirement only applies during ongoing Continuous Monitoring (post-authorization). CSPs must conduct a test of the IRP prior to achieving a FedRAMP Authorization, and at least annually thereafter as part of Continuous Monitoring.

2.5.9. Attachment 9: Control Implementation Summary (CIS) Workbook

CSPs are required to submit a CIS Workbook as Attachment 9 to the SSP. FedRAMP provides two CIS Workbook templates: one for Low and Moderate systems and one for High systems. Both are available on the FedRAMP Templates website.

In addition to a CIS worksheet tab, the CIS Workbook template includes a Customer Responsibility Matrix (CRM) worksheet tab. CSPs must use the CRM to describe the specific elements of each control where the responsibility lies with the customer. This must be done for any control with a control origination of:

- Configured by Customer (Customer System Specific)
- Provided by Customer (Customer System Specific)
- Shared (Service Provider and Customer Responsibility)

> **TIP:** Agencies rely on the CIS Workbook to understand the scope and nature of customer-specific responsibilities. Oftentimes, it is the first document opened by the AO (or designee) when reviewing an authorization package. For this reason, it is critically important to ensure that the information in the CIS Workbook is accurate and consistent with the SSP. Before submitting the authorization package, set aside time to conduct a crosswalk between the SSP and CIS Workbook. This will go a long way towards preventing delays during the review process.

2.5.10. Attachment 10: Federal Information Processing Standard (FIPS) 199 Categorization Report

CSPs are required to complete the FIPS 199 Categorization Report Template, embedded as Attachment 10 in Section 15 of the FedRAMP SSP Template. (A separate attachment is not required.) Instructions for completing the FIPS 199 Report are included in the template.

The FIPS 199 analysis represents the information type and sensitivity levels of the CSP's cloud service offering (and is not intended to include sensitivity levels of Agency data). Customer agencies are expected to perform a separate FIPS 199 analysis for their own data hosted in the CSP's cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

2.5.11. Attachment 11: Separation of Duties Matrix

Security control AC-5 requires CSPs to establish and document separation of duties for individuals that have technical, operational, or management responsibility for the CSO. Separation of duties can be documented in the AC-5 control implementation statement. CSPs also have the option to provide a Separation of Duties Matrix as Attachment 11 of the SSP.

2.5.12. Attachment 12: FedRAMP Laws and Regulations

The FedRAMP Laws and Regulations Template provides a single source for all laws, regulations, standards, and guidance applicable to FedRAMP. There is nothing for the CSP to complete. Simply download the template and include it as Attachment 12 to the SSP.

2.5.13. Attachment 13: FedRAMP Integrated Inventory Workbook (IIW)

Security control CM-8 requires CSPs to develop and document an inventory of system components within the authorization boundary that is at the level of granularity deemed necessary for tracking and reporting. To this end, FedRAMP provides an Integrated Inventory Workbook Template that CSPs must complete and submit as Attachment 13 of the SSP. Instructions for completing the IIW are provided in the template.

> **NOTE:** The IIW provides the complete listing of system components within the scope of testing, as defined in the Security Assessment Plan (SAP). 3PAOs are instructed NOT to embed or attach the IIW to the SAP. Instead, 3PAOs should simply reference SSP Attachment 13 in the Scope section of the SAP.
>
> If additional components are discovered during testing, the Security Assessment Report (SAR) must describe the deviation from the SAP. Both the SSP and Integrated Inventory Workbook must be updated to reflect the additional component(s) prior to authorization.
>
> CSPs are also required to update the IIW as part of monthly Continuous Monitoring efforts.

3.0 Security Assessment Plan (SAP)

The SAP is developed and delivered by the 3PAO. It describes the scope, methodology, test plan, and rules of engagement for the assessment of a CSO. The CSP and 3PAO are required to sign the SAP, which indicates acknowledgement of and agreement with the SAP and rules of engagement. CSPs should carefully review the SAP for quality and completeness and work with the 3PAO to make adjustments, as needed, before the assessment begins. We have provided some "checklist" guidance in this section to help CSPs when performing a review of the SAP.

Table 5. FedRAMP Security Assessment Plan (SAP) Artifacts

- SAP*
- Security Test Case Procedures*
- Penetration Testing Plan and Methodology
- Rules of Engagement (embedded in SAP)*
- Sampling Methodology

** Document must be submitted in the FedRAMP-provided template*

- Did the 3PAO use the FedRAMP template to prepare the SAP and document the Security Test Case Procedures? Current templates can be found on the FedRAMP Templates website.
- Are all required artifacts, listed in the **Table 5** above, included with the SAP?
- Does the scope accurately reflect all system services, components, and devices that comprise the authorization boundary for the system?
- Does the 3PAO intend to use a sampling methodology? If so, was the methodology included as an appendix to the SAP? For vulnerability scans, the 3PAO's sampling methodology must align with the FedRAMP Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans.
- Does the Test Schedule reflect the agreed upon schedule?
- Is the Penetration Test Plan and Methodology document consistent with the FedRAMP Penetration Test Guidance?

4.0 Security Assessment Report (SAR)

The SAR documents the results of the security assessment for the CSO, including a summary of the risks remaining at the conclusion of the assessment. The purpose of the security assessment is to evaluate the CSO's implementation of, and compliance with, FedRAMP baseline security controls.

3PAOs are responsible for developing the SAR, which is likely to go through several iterations to reflect any risks that are remediated or mitigated by the CSP during the assessment phase. CSPs should carefully review the final SAR for quality and completeness before it is delivered to the AO. We have provided some "checklist" guidance in this section to help CSPs when performing a review of the SAR.

Table 6. Security Assessment Report (SAR) Artifacts

- SAR*
- Risk Exposure Table (RET)*
- Security Test Case Procedures*
- Infrastructure Scan Results
- Database Scan Results
- Web Application Scan Results
- Penetration Test Report
- Evidence collected during the assessment

** Document must be submitted in the FedRAMP-provided template*

- Did the 3PAO use the FedRAMP template to prepare the SAR, including the RET and Security Test Case Procedures? Current templates can be found on the FedRAMP Templates website.
- Are all required artifacts, listed in the **Table 6** above, included with the SAR?
- Verify that all findings in the Security Test Case Procedures Workbook (also known as the "Test Case Workbook") are documented in the SAR.
    - To do this, look at the "CtrlSummary" tab in the Test Case Workbook. All instances of controls with an assessment result of "Other than Satisfied" should be documented as an open risk in the RET, unless the finding was corrected during testing. If the finding was corrected during testing, it should be documented in Table 5-1 of the SAR, *Risks Corrected During Testing*.
- Did the 3PAO adequately describe the mitigating factors for the risks listed in Table 5-2, *Risks with Mitigating Factors* (also known as "Risk Adjustments")? AOs tend to look very closely at the mitigating factors, particularly for risks with an initial rating of High.
- Did the 3PAO adequately describe the rationale and mitigating factors for the risks listed in Table 5-3, *Risks Remaining Due to Operational Requirements*? AOs also look very closely at the rationale and mitigating factors for ORs.
- Is the high-level summary of risks in Section 7, *Authorization Recommendation*, consistent with the RET?
- Is the detailed breakdown of risks in Appendix F, *Assessment Results*, consistent with the RET?
- Are all other appendices completed in accordance with the instructions?
- Did the 3PAO attest to the accuracy of the SAR and provide an authorization recommendation in Section 7, *Authorization Recommendation*?

5.0 Plan of Action and Milestones (POA&M)

Security control CA-5 requires CSPs to develop a Plan of Action and Milestones (POA&M) to document remediation plans for correcting risks (e.g., weaknesses, deficiencies, vulnerabilities) identified during security assessments and Continuous Monitoring activities.

CSPs are required to use the FedRAMP POA&M Template to track and manage risks. Instructions for completing the POA&M Template are provided in the POA&M Template Completion Guide.

CSPs are required to submit a POA&M with the initial authorization package. Before authorizing the CSO, AOs will review the POA&M to understand the current risk posture. Depending on the AO's risk tolerance, the CSP may be required to remediate or mitigate open risks prior to authorization. We have provided some general "POA&M management" guidance in this section, but CSPs should also review the following FedRAMP documents, which provide comprehensive guidance related to Continuous Monitoring:

- Continuous Monitoring Strategy Guide
- Continuous Monitoring Performance Management Guide
- Vulnerability Scan Requirements
- Vulnerability Scanning Requirements for Containers
- Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans
- Significant Change Policies and Procedures

5.1. General POA&M Guidance

- The POA&M submitted with the initial authorization package must correspond to the Risk Exposure Table (RET) in the SAR. That is, for every risk identified in the RET, there must be a corresponding POA&M item.
    - 3PAOs may combine risks associated with the use of unauthorized external services into a single risk in the RET. This is acceptable if the 3PAO determines the risk impact level is the same for all services. However, CSPs must create unique POA&M items to track each unauthorized service because remediation plans and mitigating factors will likely differ for each service.
- All open risks must be captured on the Open Items tab, even if they are not considered past due.
    - During Continuous Monitoring, CSPs are only required to capture and track past due scan-related risks in the POA&M. However, all risks identified during the 3PAO security assessment must be captured in the POA&M submitted with the initial authorization package.
- POA&Ms remediated *after* the SAR was delivered by the 3PAO should be listed on the Closed Items tab. These risks will be validated as closed by the 3PAO during the Annual Assessment.
- When creating each POA&M item, be sure to include the Identifier listed in Column A of the RET (e.g., V1-SC-13) for traceability. This can be done by simply using the RET Identifier as the POA&M Unique Identifier. Alternatively, you can add the corresponding RET Identifier to Column Z (Comments) of the POA&M.
- A Risk Adjustment (RA) is a reduction in the scanner-defined risk level of a vulnerability. To justify a RA, CSPs must describe mitigating factors or compensating controls in place that reduce likelihood and/or impact of exploitation. For RAs validated by the 3PAO during the assessment, select "Yes" in

Column U (Risk Adjustment). For RAs that were not validated by the 3PAO, select "Pending" in Column U. Pending RAs must be approved by the AO prior to authorization.

- A False Positive (FP) occurs when a vulnerability is identified that does not actually exist on the system. For FPs validated by the 3PAO during the assessment, select "Yes" in Column V (False Positive) and move the risk to the Closed Items tab (validated FPs are not considered open risks). For FPs that were not validated by the 3PAO, select "Pending" in Column V. Pending FPs must be approved by the AO prior to authorization.
- An Operational Requirement (OR) is a finding that cannot be remediated, often because the system will not function as intended, or because a vendor explicitly indicated it does not intend to offer a fix to their product. FedRAMP will not approve an OR for a High vulnerability; however, CSPs may mitigate the risk. For ORs validated by the 3PAO during the assessment, select "Yes" in Column W (Operational Requirement). For ORs that were not validated by the 3PAO, select "Pending" in Column W. Pending ORs must be approved by the AO prior to authorization.
    - Approved ORs are still considered open risks. They must be captured on the Open Items tab and periodically reassessed by the CSP.
- A Vendor Dependency (VD) exists when the CSP must rely on a downstream vendor to resolve a vulnerability, such as a patch for a commercial off-the-shelf (COTS) product, but the vendor has not yet made the fix available.
    - VDs are not considered deviation requests and do not require approval.
    - High-risk VDs must be mitigated to a Moderate level through compensating controls within 30 days.
    - VDs are tracked as open risks, and CSPs are required to check in with the vendor at least once a month to determine the status of the patch/fix.
    - When capturing risks as VDs in the POA&M, select "Yes" in Column P (Vendor Dependency), enter the last check-in date in Column Q (Last Vendor Check-in Date), and enter the product name in Column R (Vendor Dependent Product Name).

> FedRAMP requires Critical and High risks to be remediated within 30 days of discovery, Moderate risks within 90 days of discovery, and Low risks within 180 days of discovery.

POA&M Do's and Don'ts

Do's	Don'ts
• **Do** follow the instructions in the POA&M Template Completion Guide to ensure the POA&M is completed correctly. This will prevent delays during the review process. • **Do** remediate or mitigate all High risks identified during the security assessment. FedRAMP will not issue a "FedRAMP Authorized" designation on the Marketplace if there are open High risks. • **Do** ensure that POA&M items can be easily mapped to the SAR Risk Exposure Table. • **Do** provide evidence of vendor interactions regarding the status of patches/fixes (e.g., vendor notifications, email exchanges). • **Do** ensure that the information in Column E (Weakness Detector Source) is consistent with the information in the RET "Source of Discovery" column.	• **Don't** wait until the CSO is authorized before checking in with vendors on the status of patches/fixes. CSPs should conduct Continuous Monitoring activities, such as vendor check-ins, while the AO is reviewing the authorization package. Update Column Q (Last Vendor Check-in Date) to reflect the last check-in date. • **Don't** put VDs and ORs on the Closed Items tab of the POA&M. VDs and ORs are considered open risks that must be tracked by the CSP.