CSP AUTHORIZATION PLAYBOOK

GETTING STARTED WITH FEDRAMP

July 2018

FedRAMP

REVISION HISTORY

Date	Version	Page(s)	Description	Author

TABLE OF CONTENTS

LIST OF FIGURES

1.0 GETTING STARTED: IS FEDRAMP RIGHT FOR YOU?

If you have a Cloud Service Offering (CSO) that is in use by the federal government, you should be thinking about obtaining a FedRAMP authorization. Per an OMB memorandum, cloud services that hold federal data must be FedRAMP authorized.

There are two paths for pursuing a FedRAMP authorization; Joint Authorization Board (JAB) and Agency. Both authorization paths require a security assessment based on FISMA requirements and NIST 800-53 baselines, and both are explained in greater detail in the following sections. In making your business decision regarding the type of FedRAMP authorization that is most suitable for your service, it is important to consider your overall strategy for the federal marketplace. If you are brand new to the federal arena, 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 customer base. Conversely, if you already have a federal footprint and are looking to expand, a FedRAMP authorization can be a business development driver as it provides cross-government visibility in the FedRAMP Marketplace.

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 customers are asking you to obtain a FedRAMP authorization.
- You are looking to expand your business 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.

> ***Note:*** *This CSP playbook is designed as a mirror document to the Agency Playbook for Authorization. Guidance and content reflects the agency authorization process from the perspective of a CSP.*

2.0 PARTNERS IN THE AUTHORIZATION PROCESS

2.1. FedRAMP PROGRAM MANAGEMENT OFFICE (PMO)

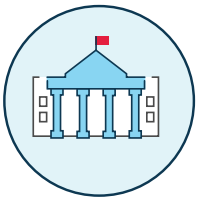
Responsible for providing a unified process for stakeholders, the FedRAMP PMO is a key partner for CSPs researching or seeking a FedRAMP authorization for their CSO. Its responsibilities include provision and stewardship of the FedRAMP authorization and continuous monitoring (ConMon) processes for Agencies, CSPs, and assessing organizations; coordination with the JAB to prioritize vendors to achieve the JAB Provisional Authority to Operate (P-ATO); project management support for CSPs and Agencies; and enabling services to be reused across government by providing a secure repository of FedRAMP authorizations.

2.2. 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), General Services Administration (GSA), and Department of Defense (DoD). The JAB defines and establishes the FedRAMP baseline system 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 on a bi-annual basis. During the prioritization process, the JAB aims to authorize cloud services it believes are most likely to be leveraged government-wide (more information about the JAB's Prioritization Criteria can be found in section 4.1 of this document). For CSOs that achieve a P-ATO, the JAB also ensures those systems maintain an acceptable risk posture through continuous monitoring.

2.3. AGENCIES



CSPs that make a business decision to work directly with an Agency to pursue an Authority to Operate (ATO) will partner with the Agency throughout the acquisition and FedRAMP authorization process. Within the 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 also conduct continuous monitoring of each authorized system, reviewing monthly and annual deliverables provided by CSPs.

Additionally, multiple Agencies using the same FedRAMP authorized system may participate in continuous monitoring collaboration groups.

2.3.1. Agency Authorizing Official

An Agency's AO is ultimately responsible for making a risk-based decision to grant a CSP's cloud service an ATO for the Agency. 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.

2.4. 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, the third party assessor must be an approved 3PAO. 3PAOs are accredited by the American Association for Laboratory Accreditation (A2LA) to provide an independent assessment. For the Agency authorization process, a CSP's Agency partner may choose to use their Independent Verification and Validation (IV&V) organization to assess the system. Once engaged, assessors are responsible for developing a Security Assessment Plan (SAP), conducting the security assessment, and developing a Security Assessment Report (SAR).

3.0 DETERMINING YOUR AUTHORIZATION STRATEGY

We recommend that you evaluate the below factors to determine your authorization strategy. Typically, CSPs are most successful when they pursue a multi-pronged approach. Before finalizing a FedRAMP authorization strategy, the PMO recommends CSPs participate in an intake call with our technical and government SMEs for a consultation. Sign up for an intake call by filling out this form.

3.1. DEMAND: BROAD vs. NICHE

Demand is a key consideration for CSPs deciding between pursuing a JAB P-ATO, Agency ATO, or both. FedRAMP generally evaluates CSOs as having broad or niche demand, where *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 RFI/RFP/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.*

3.2. EXISTING OR POTENTIAL AGENCY PARTNERS

The first step in achieving a FedRAMP Agency ATO is for a CSP to establish a partnership with an Agency. Some CSPs may already have an Agency or Agencies that are interested in authorizing their CSO, either because they are 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.

3.3. 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 correlated 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.

3.3.1. 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 SP 199

3.3.2. Impact Levels

Low Impact Level	Low impact 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 that 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. Additionally, information on the security controls involved in FedRAMP's Low Baseline can be found here.
Moderate Impact Level	Moderate impact systems accounts for nearly 80% of CSP services that receive FedRAMP authorization and 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. Information on the security controls involved in FedRAMP's Moderate Baseline can be found here.
High Impact Level	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 government's most sensitive, unclassified data in cloud

	computing environments, including data that involves the protection of life and against financial ruin. Figure 1 below illustrates the distribution of High Baseline cloud services across the federal government. Information on the security controls involved in FedRAMP's High Baseline can be found here.

CSPs must correctly align their CSOs to an impact level to pursue the appropriate authorization baseline. For example, it would not be appropriate for CSOs that qualify for LI-SaaS or align with Low Baseline to pursue a JAB P-ATO. Rather, a JAB P-ATO would be better suited for cloud services that are moderate and high impact. CSPs should use the FedRAMP FIPS 199 Categorization Template 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.

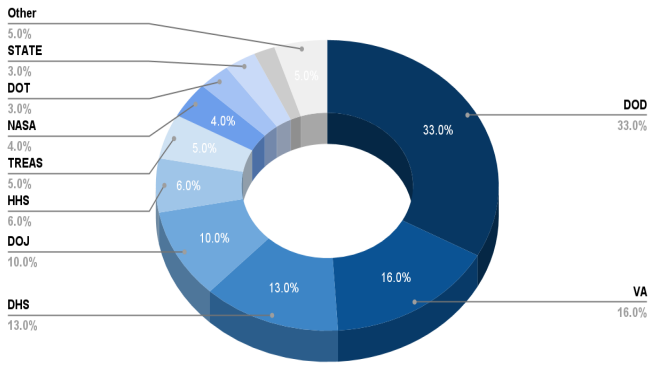


Figure 1: High Baseline Across the U.S. Government

3.4. DEPLOYMENT MODEL

CSPs should be able to qualify whether their CSO is government-only or exists as a public cloud.

Federal Government Only Cloud	Only federal government customers are allowed to use these clouds. Federal government-only cloud presents less risk to government customers and is a prioritization criterion for the JAB.
Government Only Cloud	The cloud holds only government data. Customers can be federal, state, local, tribal, territorial, federally funded research centers (FFRDCs), or lab entities.
DoD Only Cloud	The cloud holds only DoD data. Theses clouds are best suited for Agency authorizations, as the JAB is meant for cloud services that have wide applicability.
Public Cloud	Public cloud deployments support both government and non-government customers. This aligns with the traditional model of cloud computing services, but it poses more of a risk to the federal government.
Private Cloud	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.

4.0 TYPES OF FEDRAMP AUTHORIZATIONS

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

4.1. JAB AUTHORIZATION

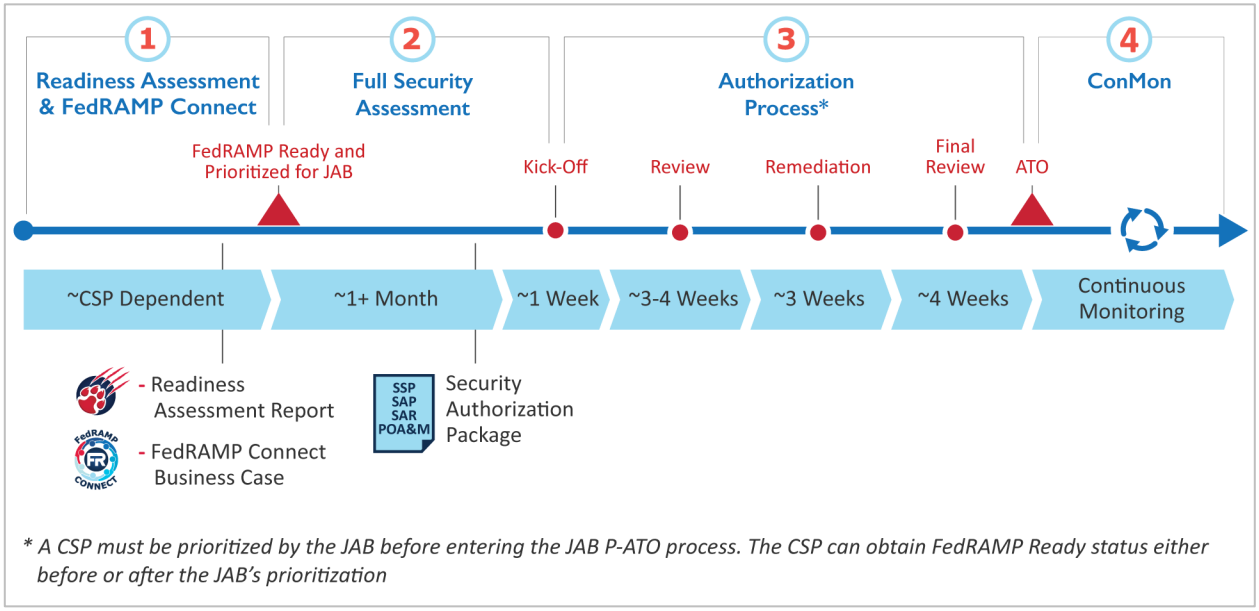


Figure 2: JAB Authorization Process Map

4.1.1. Phase 1: FedRAMP Readiness Assessment and FedRAMP Connect

FedRAMP Connect

The JAB invests heavily in creating a broad marketplace of providers and, based on current resources and funding, only has the capacity to authorize a limited number of CSOs a year. To ensure a clear return on investment of the resources used to authorize CSOs for the US 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 only mandatory prioritization criteria for vendors is demonstrated demand for their service by a wide variety of federal government Agencies. 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 service from Agencies. Three types of customers the FedRAMP PMO looks for are 1) current customers of the CSO, 2)

current federal customers using either an on premise or commercial version of the CSO, and/or 3) potential Agency customers who are actively interested in the CSO. The demand verification provided by potential Agency customers does not bind them in any way to procure the CSP's service; it is merely a demonstration of active interest and a potential procurement if the CSO was to receive a JAB P-ATO.

The JAB prioritizes six (6) vendors twice 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 detailed in Figure 2.

FedRAMP Readiness Assessment Report

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, achieving FedRAMP Ready status indicates a greater likelihood of success in the authorization process as the government has a clearer understanding of a CSP's technical capabilities. Additionally, a FedRAMP Ready designation is weighted heavily during the FedRAMP Connect evaluation and prioritization process. When planning for the FedRAMP authorization process, CSPs should consider that FedRAMP Ready status is only valid for one calendar year after designation from the FedRAMP PMO.

To achieve the FedRAMP Ready designation, a CSP must partner with an accredited 3PAO to complete a readiness assessment of its service offering. 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 reviewed by the FedRAMP PMO within one business week of submission. If there are any issues spotted by the PMO in the review, an in-person meeting is held to discuss the PMO's comments and what is needed in order for the CSP to be deemed FedRAMP Ready. Once the PMO approves a RAR, the CSO will be designated FedRAMP Ready and advertised as such on the FedRAMP Marketplace. In addition to being required to pursue a JAB P-ATO, being advertised 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 RAR engagement with a 3PAO. CSPs should not expect to be deemed FedRAMP Ready the first time they do a self-assessment or have an assessment performed by 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.

4.1.2. Phase 2: 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 an accredited 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 Actions 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-provided templates and submitted together. The FedRAMP PMO 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 two weeks prior to a kick-off meeting with the JAB. The FedRAMP PMO will then work with the CSP and 3PAO to conduct a completeness check and coordinate the JAB kick-off meeting.

4.1.3. Phase 3: Authorization Process

The first step of the Authorization Phase is to hold a kick-off meeting with the JAB, FedRAMP PMO, the 3PAO, and the CSP's authorization team. The purpose of the kickoff is to conduct a collaborative deep dive into the service offering, system architecture, security capabilities, and risk posture, typically through a combination of briefings and informal Q&A. The outcome of the kickoff will be a "go" or "no-go" decision to proceed with the authorization phase. CSPs can be exited (no-go decision) from the process for any number of reasons; 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 kick-off 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, 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 delivery must coincide with the authorization package delivery, two weeks prior to the kick-off meeting. The second ConMon delivery must occur within 30 days of the first, and establishes the CSP's normal monthly delivery date. Subsequent ConMon deliveries 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 authorization of their CSO from the FedRAMP PMO.

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 role and responsibilities within the JAB P-ATO authorization process can be found here.

4.1.4. Phase 4: Continuous Monitoring

Following issuance of a JAB P-ATO, the CSP is required to *maintain* a security posture that aligns with FedRAMP and the JAB'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 systems with JAB P-ATOs, the FedRAMP 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, and
- 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 employ a 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.

4.2. AGENCY AUTHORIZATION

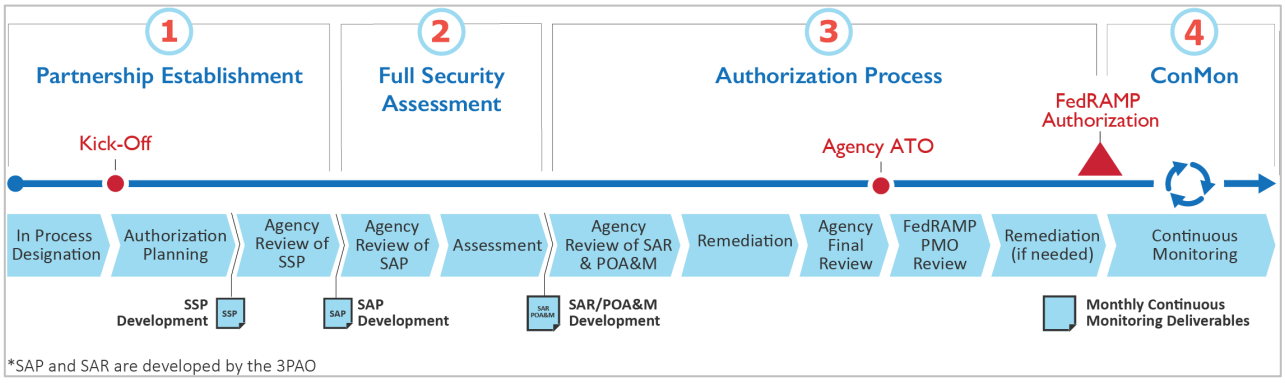


Figure 3: Agency Authorization Process

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 the CSP would complete and accounts for steps that the agency would complete.

4.2.1. Phase 1: Partnership Establishment

In the partnership establishment phase, a CSP formalizes their partnership with an agency via FedRAMP's In Process requirements. In some cases, a vendor may be under contract with an Agency already, or an Agency may be working through the acquisition process. By this stage, a CSP should have a system that is fully built and functional, and a leadership team that is committed and fully on board with the FedRAMP process. Additionally, if they have not already done so, a CSP should engage with the FedRAMP office through the intake process.

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. FedRAMP has Requirements for Obtaining an In Process Designation, which outline the requirements for achieving this designation. Once In Process, CSPs are displayed on our FedRAMP Marketplace as such.

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 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, who will do their own FIPS 199 assessment.

Throughout this phase, a CSP will be working on the development of their System Security Plan (SSP), which is the security blueprint of their system. This robust document outlines how their system security aligns with the FedRAMP controls. While the SSP does not need to be complete prior to establishing a partnership with an agency, it does need to be complete and fully reviewed by the agency prior to Phase 2. The agency partner should approve and sign off on the SSP prior to beginning testing.

Though it is not required, a CSP may choose to hire a consultant to help them develop their FedRAMP documentation if they do not have this expertise in house. If a CSP chooses a consultant from the

approved list of FedRAMP 3PAOs, they must ultimately select a different 3PAO for their testing to ensure that independence is maintained.

Once the partnership is established, a CSP should:

- Develop an initial project plan that maps out the various milestones associated with the authorization
- Confirm resources dedicated to the authorization process. At a minimum this should include one technical writer, one technical SME, and one project manager
- Work with the Agency to select a 3PAO for the assessment in Phase 2. While CSPs can utilize other independent assessment organizations for Agency ATOs, FedRAMP strongly recommends the use of a FedRAMP-accredited 3PAO.
- Complete FedRAMP Training, including the mandatory training: FedRAMP System Security Plan (SSP) Required Documents (200-A).
- Contact the PMO at info@fedramp.gov for access to FedRAMP's secure repository.

The final step in this phase is to prepare for and conduct a kick-off meeting. During the kick-off meeting, a CSP and Agency will:

- Understand roles and responsibilities of all project team members including Agency, CSP, and 3PAO personnel
- Review project schedule and milestones and gain consensus from all parties
- Ensure that all parties have access to FedRAMP's secure repository to obtain FedRAMP deliverables
- Review network topology, interconnections, and system boundary diagram
- Discuss and gain consensus on any additional Agency requirements, as well as any other Agency-specific security concerns

> 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 the Authorizing Official, who is required to send a note 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 help.

4.2.2. Phase 2: Full Security Assessment

Prior to beginning Phase 2, a CSP should ensure that:

- The SSP is complete and has been reviewed and approved by their Agency partner
- The Security Assessment Plan (SAP) has been developed by their 3PAO with their input

During this phase, the 3PAO tests the CSP's system. 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 Security Assessment Report (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.

4.2.3. Phase 3: 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 Authority to Operate (ATO) letter signed by the Authorizing Official.

Once an ATO letter has been signed by an Authorizing Official, the Agency or CSP should upload the entire security package (SSP and attachments, SAP, SAR, POA&M), along with the FedRAMP checklist and ATO letter, to FedRAMP's Secure Repository on OMB MAX. They should also e-mail info@fedramp.gov when this is complete to prompt the PMO to conduct their review. If possible, the CSP should provide advance notice that the package will be uploaded to help expedite the PMO's review. The PMO then conducts a two-phased review of the package that is focused on collaboration early on with the agency, CSP, and 3PAO:

- Phase One focuses on the basic technical security posture of the service offering and consists of the review of the authorization boundary, data flow, critical control implementation, and security assessment results
- Phase Two focuses on the full review of the agency package and any gaps identified during Phase 1

After the Phase One review, which typically takes less than a week, the PMO meets with the CSP, 3PAO, and Agency to share their findings. The CSP is given the opportunity to address any issues that must be rectified in order to achieve FedRAMP Authorization. The PMO will shift to the Phase Two review once any findings from the Phase One review are addressed. FedRAMP will make a decision for FedRAMP Authorization, pending the Phase 2 review.

Once a CSP is deemed FedRAMP Authorized, a CSP is reflected as such on the FedRAMP Marketplace, and FedRAMP makes their security package available, upon request and validation of the requestor, to the entire federal government for the purpose of issuing their own ATO for the use of the service. Due to the sensitivity of the materials, this information is highly controlled through the use of an access request form that must be routed through appropriate signatures within the federal government. Each form requires FedRAMP's approval to review the documents.

> Once a cloud service has achieved the FedRAMP Authorization designation, each subsequent agency customer must still provide their own ATO for the use of the service. The agency has 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 PMO can support calls to discuss it. All ATO letters should be sent to FedRAMP for monitoring.

4.2.4. Phase 4: 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 typically include, but are not limited to an updated POA&M, scan results/reports, system change information/requests, as agreed upon between the Agency and the CSP. Each Agency using the service reviews the monthly continuous monitoring deliverables, but do not need to be shared with FedRAMP. CSPs may use the FedRAMP repository for posting monthly continuous monitoring material for ease of access and sharing with Agency representatives.

Once a CSP has multiple Agencies using their FedRAMP Authorized service, the PMO recommends that a vendor host monthly continuous monitoring collaboration calls. The purpose of these calls is to gain a better understanding of agency concerns and questions regarding the security of their system, and to get updates from the CSP on continuous monitoring status as well as any important concerns/issues about the service. This can streamline any work that the CSP needs to do with regard to continuous monitoring, and can help disperse the responsibility across partner agencies.

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.

5.0 IMPORTANT CONSIDERATIONS

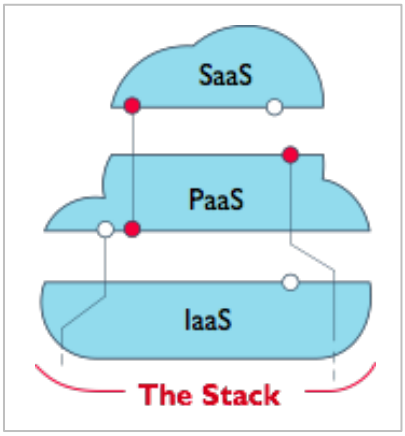
Below are some areas of consideration as you develop your authorization strategy. We recommend you understand these areas and be prepared to talk about them during your intake call with the FedRAMP PMO.

5.1. 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:

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).

5.2. 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) has its own authorization boundary and its own ATO letter.

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 and authorize the entire stack. The CSP is responsible for the entire stack in this situation and details the underlying infrastructure and platform within its system security plan (SSP). The authorization in this case, would be for the SaaS with it's own infrastructure, but the infrastructure itself would not constitute an Infrastructure as a Service (IaaS).

The FedRAMP PMO highly recommends that CSPs discuss to 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 is here); however, this is not required for an Agency authorization.*

5.3. LEVEL OF EFFORT

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 and cost can be broken down into the following categories:

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
- Not having FIPS 140-2 validated encryption algorithms
- Not implementing multi-factor authentication appropriately
- Poor configuration documentation and immature management processes
- Not applying appropriate resources up front (bake security and resources in early)

5.4. AUTHORIZATION TEAM

Staffing an authorization effort - JAB or Agency - 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:

Project Management	Experience with team- and task- management as part of 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 and are comfortable in the coordination of project stakeholder 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 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.