

FedRAMP strategy guide

How to approach FedRAMP holistically to maximize results

COALFIRE COMPLIANCE ADVISORY SERVICES

Table of contents

FedRAMP overview2

Strategy and executive sponsorship.....3

 The FedRAMP process for attaining an ATO can be broken down into five main steps:.....4

FedRAMP costs5

 Estimating the cost of FedRAMP5

Infrastructure-as-Code and automation6

FedRAMP timeline.....6

FedRAMP lifecycle8

 Pre-assessment (Phase 1 and Phase 2)8

 Assessment (Phase 3)9

FedRAMP assessment approach.....10

 Continuous monitoring (Phases 4 and 5)11

How Coalfire can help.....12

 FastRAMP 360 – advisory, engineering, and managed services12

 FedRAMP assessment services13

FedRAMP overview

For government agencies wishing to utilize cloud services, the Federal Risk and Authorization Management Program (FedRAMP) is at the center of governmental IT modernization. The government's Cloud Smart policy requires that federal agencies use FedRAMP-authorized solutions whenever possible to reduce costs and streamline IT procurement. The goals of Cloud Smart are to:

- Ensure common cloud service provider (CSP) security and compliance standards by awarding an Authority to Operate (ATO), which is accepted by all federal agencies.
- Utilize the "do once, use many" framework.

Thanks to structural changes in the FedRAMP program and innovations, such as automation methodologies, taking the right approach to the FedRAMP process can minimize required effort, time, and cost to achieve authorization.

Figure 1. FedRAMP program and federal market trends



Strategy and executive sponsorship

For companies considering FedRAMP, developing a holistic business strategy and obtaining executive sponsorship are critical, as they underscore a strategic direction to invest in the needs of federal clients. Significant investments in time and resources are required to complete the endeavor. In the process of developing a holistic strategy, you must address many important technical, organizational, and competitive questions to ensure organizational alignment and maximize results:

- How much will FedRAMP cost?
- What are the maintenance costs after authorization?
- What will the return on investment be?
- How many technical resources are required?
- How quickly can the service be listed in the FedRAMP marketplace?
- Who are your competitors in the FedRAMP marketplace?
- How should you differentiate your service? What is your federal sales strategy?
- How do you secure an agency sponsor?
- Does your system need to be in Azure or AWS GovCloud? Or can it remain in a commercial cloud?
- Which FedRAMP baseline should you pursue?
- Should you go the Agency Authorization or the Joint Authorization Board (JAB) path?
- What services should you go to market with?

Achieving FedRAMP ATO is an extremely detailed, complex, and multifaceted undertaking that requires involvement from the entire organization:

- Senior leaders provide the strategic vision, top-level goals, and objectives.
- Mid-level leaders plan and manage projects.
- Individuals on the frontlines develop, implement, and operate the systems that support the organization's core mission and business processes.

Your organization will need to reach beyond IT maintenance to a variety of corporate areas – such as engineering, operations, human resources, training, physical security, project management, data center operations, and vendor contracting – to present the holistic security posture to outside auditors.

Figure 2. FedRAMP key stakeholders



The FedRAMP process for attaining an ATO can be broken down into five main steps:

- 1. Consulting advisory and preparation** – Your selected advisor advises on business strategy and approach, system architecture, remediation, and documentation of the environment and security control implementations. Your advisor can also produce a system security plan (SSP), policies and procedures, and other necessary system documentation.
- 2. FedRAMP readiness assessment** – Your 3PAO conducts the required readiness capabilities assessment to determine your cloud's readiness for the full FedRAMP assessment. This step is required for the JAB path and is optional for agency paths (these paths are explained in detail in the following sections).
- 3. Pre-assessment** – Your 3PAO performs a quick "gap" analysis or inventory of your current cloud system documentation. The deliverable is a high-level roadmap of next steps with associated levels of effort for completion.
- 4. Assessment** – Your 3PAO develops the required FedRAMP documentation, including:
 - A security assessment plan (SAP), which leverages the SSP and inventory collected during the third step
 - Security requirements traceability matrix (SRTM) to document assessment results
 - Vulnerability scanning of operating systems, databases, and web application(s)
 - Penetration test report
 - Security assessment report (SAR)
 - Recommendation for authorization
- 5. Continuous monitoring** – Monthly, quarterly, and annual continuous monitoring is required to achieve and maintain the ATO.

FedRAMP costs

Historically, FedRAMP projects vary widely. Industry estimates place project costs between \$200,000 and \$5 million for environment creation, FedRAMP preparation, and FedRAMP assessment. Much of the variation of timing and price depends on the solution's size and your familiarity with compliance frameworks. If you've generated artifacts for other industry regulatory compliance or security assessments, then documents, policies, processes, and plans could potentially be reused for FedRAMP efforts.

Estimating the cost of FedRAMP

Public information regarding the cost of preparing for and achieving FedRAMP authorization is limited due to wide variability in how the private sector accounts for spending and expenses. Even though no comprehensive dataset is available to determine the average financial commitment required, our experience shows that FedRAMP costs and spending are concentrated in several areas:

- Allocation of internal resources to manage and maintain FedRAMP efforts and any required cybersecurity activities that were previously unaccounted for
- Technical remediation of information system issues
- Procurement of new or improved cybersecurity tooling and infrastructure
- Third-party advisory and preparation services
- The cost of an independent 3PAO security assessment

When calculating the overall cost of FedRAMP, you must evaluate the costs of necessary cybersecurity tooling and technical remediation required for FedRAMP, which vary widely. Obvious factors such as the overall size of the cloud service offering (hyperscale versus startup) or the complexity of system design, precluding any simple technical remediation, play a definite role in this variance and are easily incorporated into any internal financial assessment of the overall costs of FedRAMP. But three other factors have a large impact on this variance as well, regardless of size and complexity:

- Deciding whether to build a new production environment for FedRAMP or uplift current deployment
- Choosing whether to leverage an underlying Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) provider or maintain control over the entire technical "stack" of the cloud production environment
- Determining how much security automation to proactively invest in when preparing for FedRAMP

An often-forgot aspect of FedRAMP is the cost of maintaining authorization after achieving an initial ATO. FedRAMP should not be considered a point-in-time cost, but rather an ongoing operational investment. Depending on some of the factors discussed in this section, the cost of maintaining authorization can add quite a bit to initial cost estimates for undertaking FedRAMP.

Infrastructure-as-Code and automation

Recent technology advancements in Infrastructure-as-Code (IaC) and automation accelerate the ability to implement security controls, which shortens time to compliance. You can leverage automated modules and IaC that have been preconfigured to meet FedRAMP controls and requirements to speed system build and deployment, saving time and costs and shrinking overall time to market. You should proactively implement a security automation strategy to get ahead of FedRAMP requirements, decrease the overall time required to gain authorization, and reduce the cost to maintain compliance with FedRAMP and agency-specific cybersecurity requirements.

FedRAMP preparation efforts that leverage automation methodologies show great promise in reducing time to compliance and improving security as preconfigured, cloud-based, compliant security stacks.

FedRAMP timeline

There are two main paths to ATO (see Figure 3):

1. **Agency**
2. **JAB***

The agency path requires you to partner with an agency for CSP documentation review and 3PAO SAR review. The agency requires a SAR, but the readiness assessment report (RAR), which occurs in Stage 2, is optional.

The JAB path requires you to:

- Create a presentation outlining your federal customers and the security of their architecture. The JAB would like to see that you're currently working with five or more agencies before facilitating prioritization to work with the JAB.
- Complete the architecture design and security controls implementation and the required FedRAMP documentation.
- Work with a 3PAO to complete a RAR. Once the JAB approves the RAR, work with the 3PAO to complete a full assessment.

The JAB reviews the SAR and once approved, you will be awarded a Provisional Authority to Operate (P-ATO) that other agencies can leverage to use your service or offering.

A FedRAMP project can be divided into pre-assessment and assessment phases. Each phase is distinctly delineated when you complete an initiation request on your cloud system to the FedRAMP PMO, and each phase has its own set of activities.

FedRAMP has worked closely with NIST and industry organizations to develop the Open Security Controls Assessment Language (OSCAL), a standard that can be applied to the publication, implementation, and assessment of security controls.

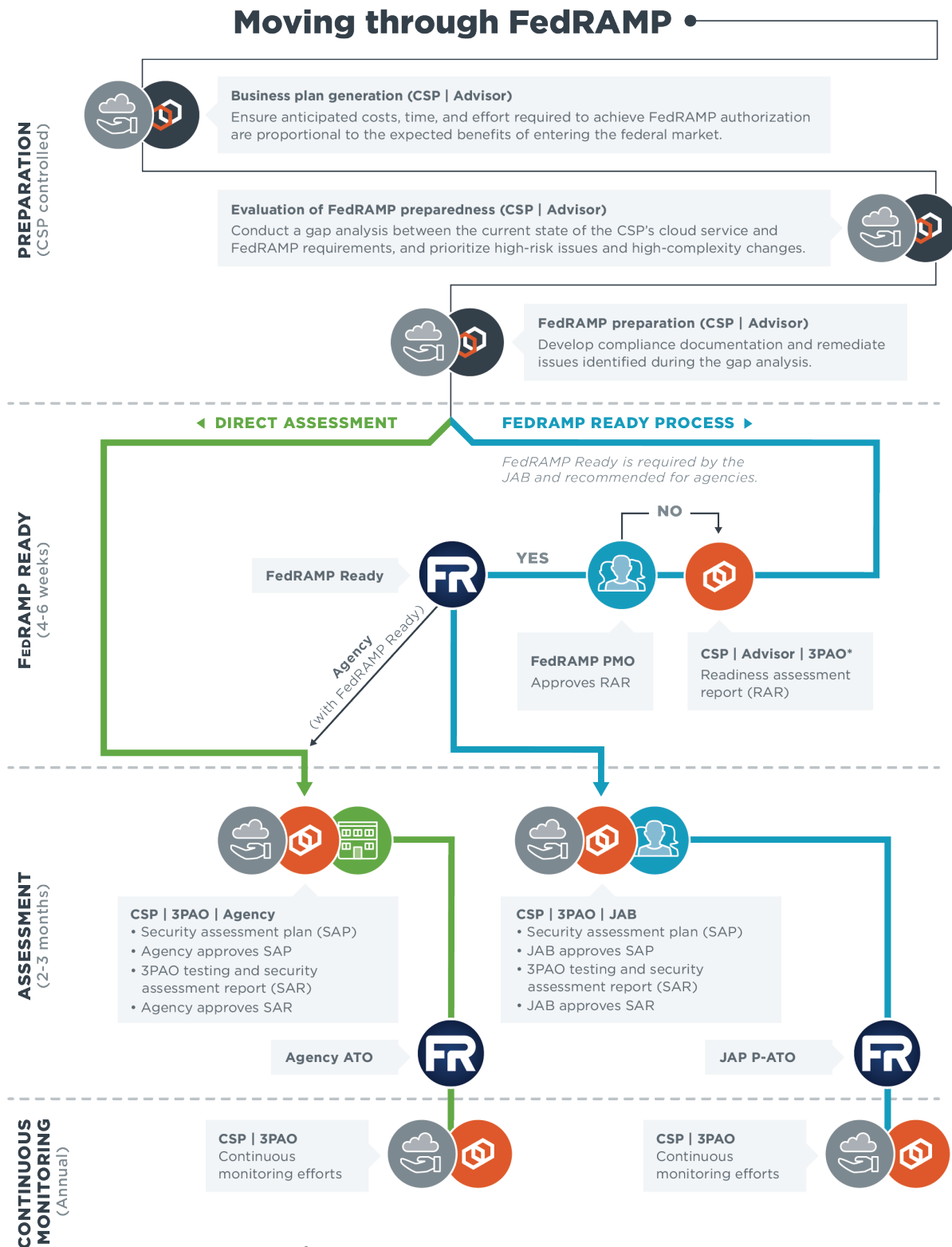
FedRAMP expects OSCAL will streamline and automate components of the authorization process.

Benefits include:

- **CSPs** will be able to create their SSPs more rapidly and accurately, validating much of their content before submission to the government for review.
- **3PAOs** will be able to automate the planning, execution, and reporting of cloud assessment activities.
- **Agencies** will be able to expedite their reviews of the FedRAMP security authorization packages.
- **The FedRAMP Program Management Office (PMO)** expects to be able to build tooling to further reduce costs and improve the quality of security reviews.

* A FedRAMP readiness assessment report (RAR) is required for the JAB path and is optional for agency path.

Figure 3. The two paths to FedRAMP ATO

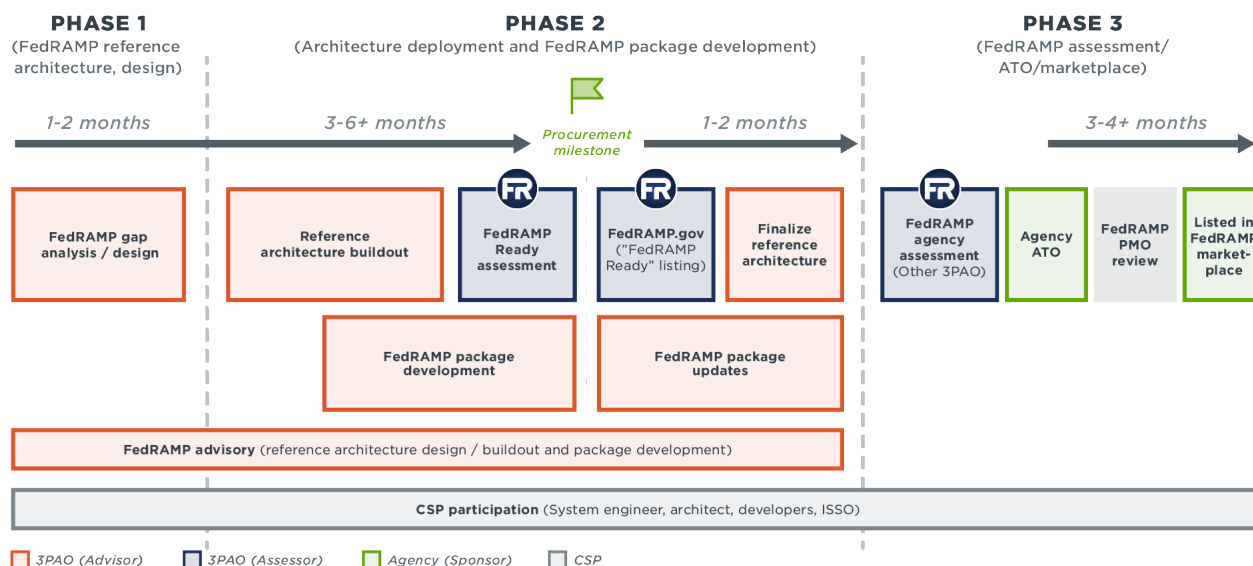


COALFIRE. | © 2021 Coalfire. All rights reserved.

*Coalfire can act as an assessor or an advisor, but a 3PAO is not allowed to play both roles for a client.

FedRAMP lifecycle

Figure 4. FedRAMP lifecycle



The diagram in Figure 4 details the FedRAMP lifecycle and the three phases from FedRAMP preparation to FedRAMP authorization. Phase 2 is sometimes the most arduous process, but it can often be shortened with automation strategies.

Pre-assessment (Phase 1 and Phase 2)

Pre-assessment is where the FedRAMP submission package is prepared and created. Steps of this assessment include:

1. Verify system boundary definitions.
2. Evaluate critical control implementation.
3. Educate stakeholders regarding final assessment requirements, timelines, and likelihood of ATO by chosen sponsor.
4. Determine whether the cloud service offering meets the FedRAMP federal mandates to become "FedRAMP Ready." All federal mandates must be met. FedRAMP will not waive any requirements.
 - Are FIPS 140-2 validated cryptographic modules consistently used where cryptography is required?
 - Can the system fully support user authentication via agency common access card (CAC) or personal identity verification (PIV) credentials?
 - Is the system operating at digital identity level 2 or higher?
 - Can you consistently remediate high vulnerabilities within 30 days, moderate vulnerabilities within 90 days, and low vulnerabilities within 180 days?

- Do you and the system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?¹
 - Does the system's external DNS solution support DNS security (DNSSEC) to provide origin authentication and integrity verification assurances?
5. Download FedRAMP templates.
 6. Decide if you will submit through FedRAMP JAB or obtain a federal agency sponsor. This decision will have significant impact on the project timeline as elaborated in the assessment phase.
 7. Create supporting policies, processes, and plans.

Upon completion of required FedRAMP documentation, the documents are submitted for 3PAO review. The 3PAO examines the most critical security controls and works with you to identify any necessary updates to FedRAMP documentation, which starts the FedRAMP assessment phase (Phase 3).

Assessment (Phase 3)

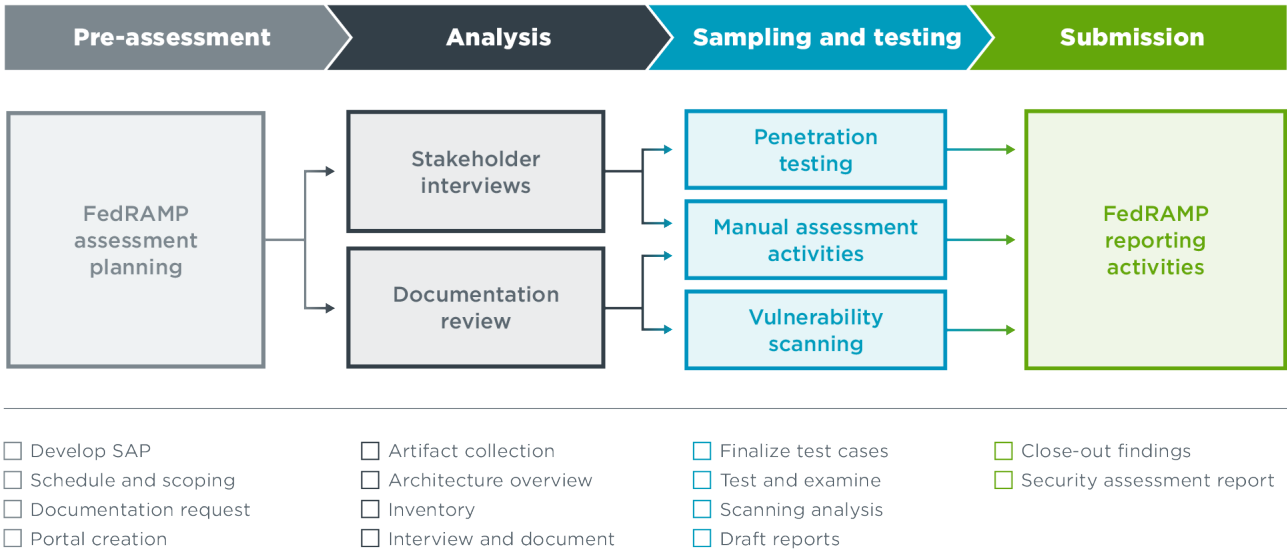
The FedRAMP assessment includes:

1. Security controls assessment against NIST SP 800-53 Revision 4 (scope dependent on the system impact level of high, moderate, or low)
 - This includes documentation review of your policies, procedures, and SSP.
 - Interviews with your personnel determine control implementation and effectiveness.
 - Testing and artifact collection ensure proof is obtained that you meet the required FedRAMP controls and control parameters.
2. Vulnerability scanning (of all operating systems, network devices, infrastructure, databases, and web applications)
3. Penetration testing
4. Source code review (required for initial FedRAMP assessment)

¹ <https://www.archives.gov/records-mgmt/grs>; PL 104-231, 5 USC 552

FedRAMP assessment approach

Figure 5. Required actions per stage

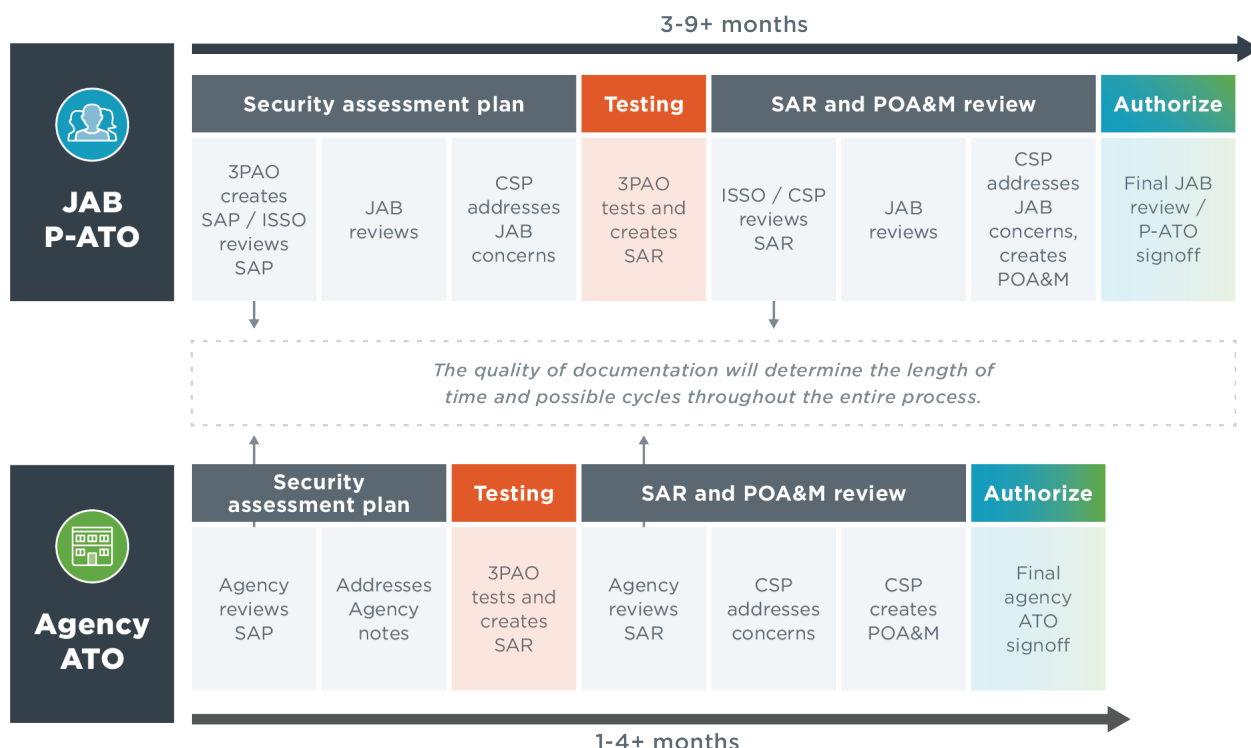


The timeframe of the assessment phase is mainly dictated by the selected path and your readiness to respond to comments throughout each stage. Figure 6 shows the process, notional timeframe, and steps to achieve the different authorization types. The biggest difference between the two is the level of security package review. Generally, the timeframes for each authorization type are:

- Agency ATOs: One to four or more months (updated for FedRAMP Accelerated timeframe)
- JAB P-ATOs: Three to nine or more months (updated for FedRAMP Accelerated timeframe)

Your security package will then be listed in the FedRAMP repository as being FedRAMP compliant. Federal agencies can review the package to determine if they would like to use the system described in the package.

Figure 6. Estimated timeframes for paths to FedRAMP ATO



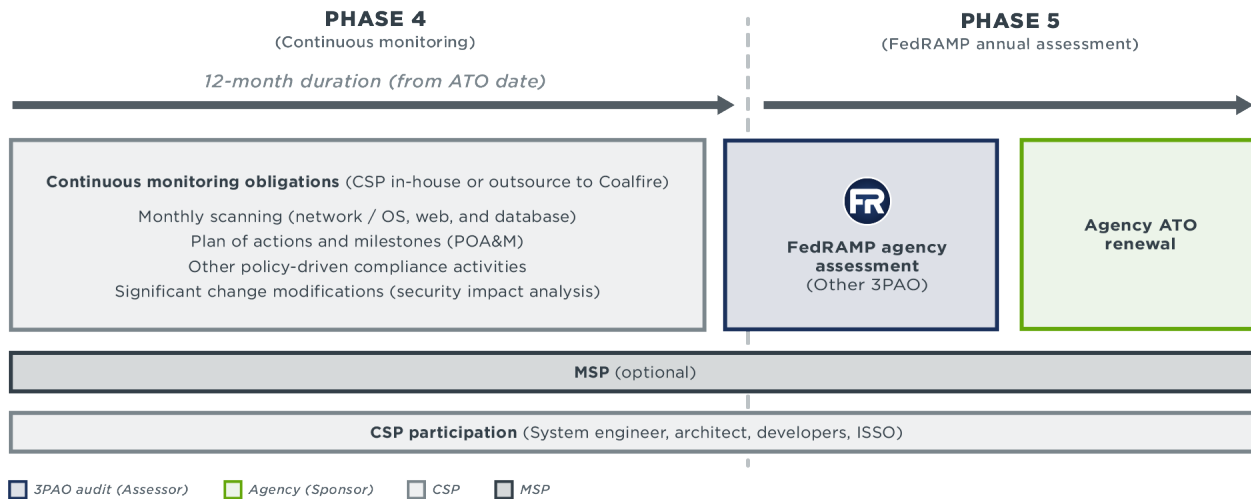
Continuous monitoring (Phases 4 and 5)

Once authorization is initially achieved, continuous monitoring activities commence. Continuous monitoring determines whether the set of deployed security controls in an information system remains effective with new exploits or attacks and planned or unplanned changes that occur in the system and its environment over time. To maintain a FedRAMP ATO, you must monitor your security control environment, assess it on a regular basis, and demonstrate that your service offering's security posture is continuously acceptable. Ongoing assessment to maintain authorization provides federal agencies using cloud services with a method for detecting changes to the system's security posture and making risk-based decisions. In general, the annual activities are:

- Periodic review of security policies, planning activities, and security procedures and processes
- Incident handling activities, including maintenance of incident records, whom it was reported to, and when it was reported
- Scanning results from infrastructure, operating systems, web applications, and databases
- Changes to the system's security posture due to changes in hardware or software on the cloud service offering or due to the discovery and provocation of new exploits

Finally, all FedRAMP authorizations must be renewed every three years. This means that all FedRAMP controls must be tested at least once every three years. The scope and frequency of the review are commensurate with the acceptable level of risk for the system.

Figure 7. Phases 4 and 5 of FedRAMP assessments



How Coalfire can help

We are the leading FedRAMP advisor and 3PAO, having directly helped more than 70% of the FedRAMP marketplace achieve and maintain ATO through a combination of consultative advisory, engineering, assessment, and cloud managed services. We provide services within the entire FedRAMP process outlined in this strategy guide.

FastRAMP 360 – advisory, engineering, and managed services

The industry's only comprehensive approach to a smarter, faster, and simplified FedRAMP journey, FastRAMP 360 incorporates consultative advisory, engineering, and managed services into one seamless approach to FedRAMP. FastRAMP 360 can be broken down into three core phases:

- **Advisory consulting** – We help you develop and align your FedRAMP business strategy to prepare your organization for the FedRAMP process. From overall strategy, competitive and market analysis through technical requirements, we ensure your organization is poised for FedRAMP success and maximized ROI from the beginning. Additionally, we advise on system architecture and documentation of the environment and security control implementations. We can produce an SSP, policies and procedures, and other required system documentation.
- **Engineering and accelerated system onboarding** – Our Accelerated Cloud Engineering (ACE) Launchpad solution deploys FedRAMP-compliant cloud architectures in just 10 days, enabling you to become audit-ready in as little as 60 days.
- **Ongoing management and optimization** – Acting as an extension of your team, our cloud managed services (CMS) minimize the operational burden on your team while drastically reducing your costs. CMS offloads the management of your FedRAMP environment from your team, reducing operating expenditures by 54% and improving your security and risk posture. As a core component of FastRAMP 360, CMS provides the peace of mind you need for continued FedRAMP success.

FedRAMP assessment services

- **Readiness assessment** – We conduct a technical capability assessment to ensure you meet the minimum requirements to achieve a FedRAMP ATO. This is required to pursue a JAB authorization. Some agencies are starting to make this a requirement as well, so ask your agency sponsor.
- **FedRAMP assessment** – We serve as the independent 3PAO to develop the 3PAO-required FedRAMP documentation, including an SAP, SRTM to document assessment results, and a SAR. This full technical assessment ensures your compliance with NIST SP 800-53 Revision 4 and FedRAMP controls. We assess manual security controls; conduct vulnerability scans on all operating systems, web applications, and databases; and perform a penetration test on your product.

To learn more about the FedRAMP process and how Coalfire can help you successfully achieve and maintain authorization, reach out to 3PAO@coalfire.com, or visit www.coalfire.com.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit Coalfire.com.

Copyright © 2021 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.

WP_FedRAMP_Strategy_Guide_102821