Preparing Your Company for FedRAMP

January 2021 | **Aaron Wilson**

ScaleSec

Table of Contents

Introduction

With the US Government spending $80B[1] on information technology last year, your commercial organization may be considering selling to federal customers. This journey can prove lucrative, but the effort to reach this new level of security and meet federal cybersecurity standards could be substantial for the uninitiated.

This paper is designed to introduce commercial companies to FedRAMP, with questions to assess your readiness to launch and maintain a federal compliance program.

Questions to Contemplate

Following are questions you might consider when preparing for FedRAMP.

If you are getting ready to pitch your product to the government, or if an agency has approached you with an interest in your product, we hope sharing some real-life experiences helps you make informed decisions early in the process.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[1] Based on data published by the US Office of Management and Budget, https://itdashboard.gov/drupal/summary/007 and US Department of Defense, https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_16_it-fy2019.pdf

What approach would bring us the fastest ROI?

The popular *minimum viable product* approach for building software can work for your approach to FedRAMP, too. If you have the luxury of attracting multiple government agencies, take the opportunity to iterate your security maturity by seeking sponsorship from an agency with less stringent security requirements. As tempting as it may be to sell to the DoD first, a federal civil, state, or local government agency with more modest data sensitivity may be a faster win, and would allow you to see a quicker return on your investment. The best sponsor for you will depend on what your product does.

Time and budget to successfully navigate this process need to be offset against the anticipated sales of your product or service to the government. The total time required depends on many factors, and 9-18 month projects are not atypical. Thankfully, much of your effort, investment, and learnings can be reused to strengthen the security of your commercial implementation. Which leads to...

How fast can we get an ATO?

Even as significant innovation is underway to meet federal compliance, many customers underestimate both the cost and time required to achieve a first Authorization to Operate (ATO). In most cases, three months is unrealistic, even though many think this is possible. FedRAMP provides publicly available data to calculate average days for the authorization process. After removing a few outliers, it's promising to see that the average duration of the authorization process has actually dropped from 430 to 172 days for the top public cloud providers.

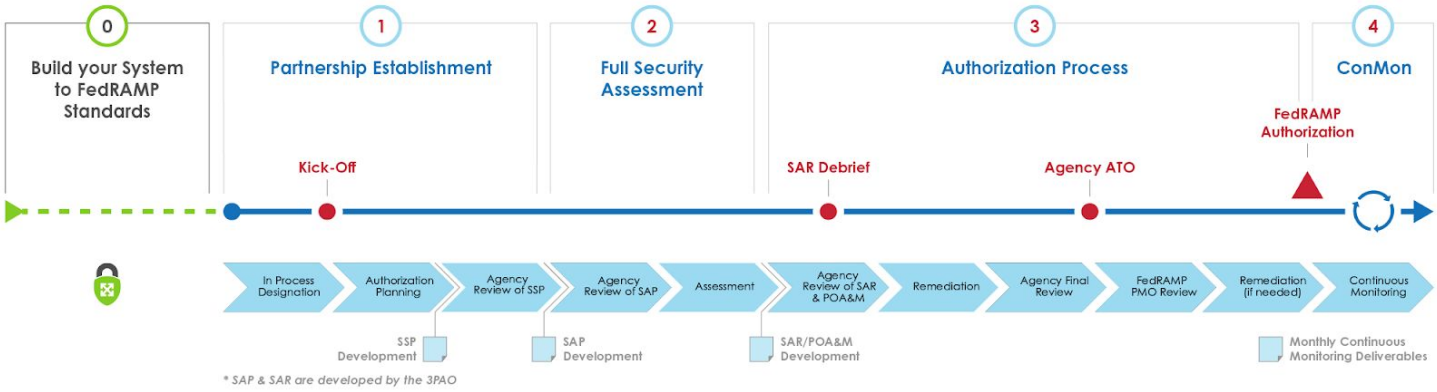
Average Days to Authorize[2]

[2] Source: FedRAMP Marketplace. Includes SaaS authorizations for AWS, Azure, and Google Cloud https://marketplace.fedramp.gov/

That's less than six months, and this is terrific progress. However, note that the start date published is the day the ATO package is received by the Agency for consideration, and after receiving approval from the FedRAMP team to begin the process.

> You still need to calculate in the time it takes to actually build the system to federal standards.

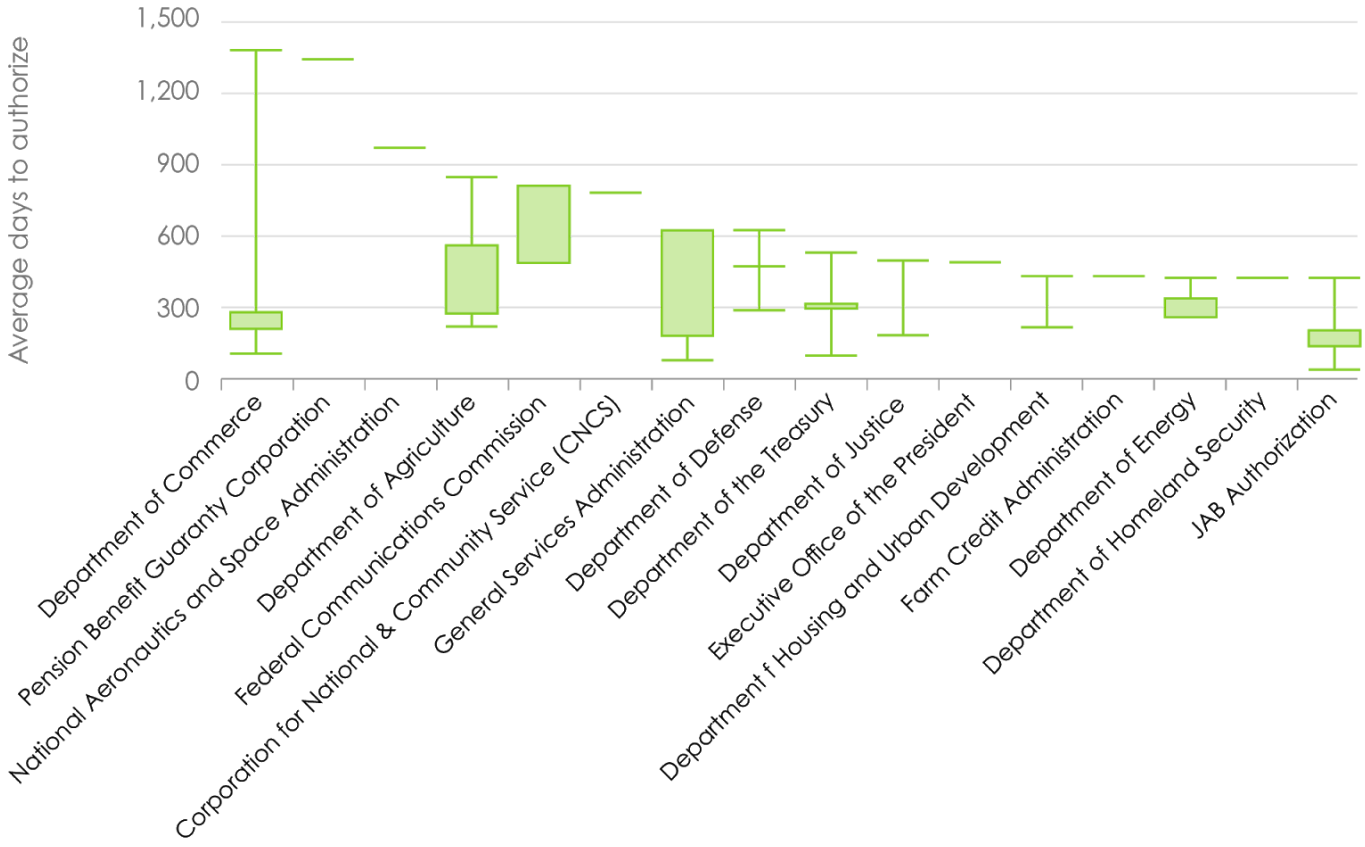
Our team refers to this project as "Phase 0," shown below with the FedRAMP Agency Authorization process diagram[3] for context.



The authorization process assumes you have built the system

[3] Source: FedRAMP Agency Authorization https://www.fedramp.gov/agency-authorization/

Further analysis of the FedRAMP Marketplace data reveals that your sponsoring agency is another factor that will determine the speed of your authorization, as shown in the graphic below:



Authorization time varies by agency

What is needed to maintain FedRAMP?

FedRAMP has ongoing costs, and it's more than a one-time technical lift. FedRAMP requires annual, quarterly, monthly, and continuous ongoing duties to maintain your authorization. The program requires an ongoing commitment to:

→ Educating key stakeholders, technical personnel, and support teams

→ Documenting and explaining a detailed understanding of your application: the underlying infrastructure, its software components, and data flows

→ Thorough understanding of your third party providers and their security capabilities, including your cloud provider

→ Establishing internal programs to meet ongoing requirements for change management, vulnerability management, security monitoring, incident response, and documentation management

→ Regular third-party system and documentation audits

Successful strategies to achieve an ATO consider these operational expenses in addition to the one-time costs. For a table of ongoing required operational activities, check out the *FedRAMP Continuous Monitoring Strategy Guide*[4].

Have we identified a sponsor (buyer) to work with us?

You can begin preparing for FedRAMP anytime, but you need a federal agency to sponsor your product to receive an authorization. You'll also need a sponsor to get your product listed on the FedRAMP Marketplace.

Establishing a strong working relationship to build and develop trust with your first sponsor is crucial for a successful relationship. These conversations will likely be iterative and ongoing as you share the features of your product that will directly benefit your sponsor's program and mission objectives.

Your sponsor will be "taking a chance on you." FedRAMP authorizations are signed by a federal employee who determines that the use of your software is worth the risks. Your ongoing relationship with them lays the foundation for the confidence needed to buy your product--and know that you will guard government data fiercely. The consequences of mishandling federal data are serious. Transparency in conversations throughout the process will help establish and maintain trust.

What kind of federal data would my product process?

Many companies are unaware that they do not get to select the system impact level for their product. FedRAMP supports four baselines[5] that match security to the data's

[4] https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

[5] Several optional and possibly mandatory layers may be needed. DoD models excluded.

sensitivity: *Tailored*, *LOW, MODERATE*, and *HIGH*. This impact level is selected based on the sensitivity of the data your product processes.

To make the most of your business opportunities, the correct impact level is crucial. Selling your product implemented as a LOW impact system may narrow opportunities. A HIGH impact level may drive your costs too high for some agencies.

For each information system (like for your product), FedRAMP uses a well-defined litmus test[6] to determine how substantial the cybersecurity protections must be. The outcome of this exercise is the primary driver for the cost and schedule.

By identifying and working with a sponsor, you will determine together the level that is right for your system based on the agency's use case.

What are staffing considerations?

A healthy FedRAMP program needs more ongoing attention than what can be accomplished by people wearing *a few more hats*. While this paper in no way covers a complete team, there are some crucial roles that are important to identify early.

Your sponsoring agency will ask you to explain how your system works and how it is managed in great detail to this person. This is done best by a representative who has experience supporting federal compliance and communicating complex cloud technology concepts. This person should also understand the FedRAMP authorization process and its requirements.

FedRAMP incorporates the 800 series NIST Special Publications[7] and requires cloud service providers to complete an independent security assessment conducted by a third-party assessment organization (3PAO). Having someone on your team or a consultant onboard who is experienced with NIST and federal compliance will substantially improve your odds of success.

While FedRAMP does not explicitly include citizenship requirements[8], agencies may have a preference. Some agencies are comfortable with offshore developers working

[6] https://csrc.nist.gov/publications/detail/fips/199/final

[7] See NIST SP 800-53a https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

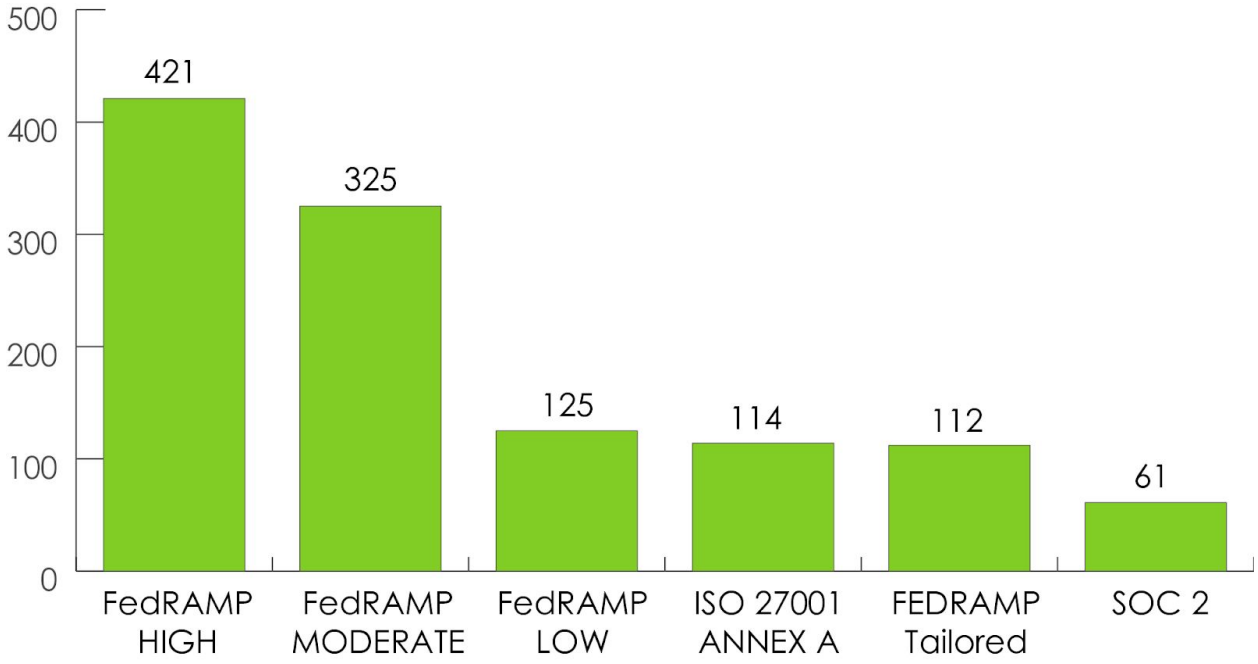
[8] The DoD version of FedRAMP does include citizenship requirements - see section 5.6.2 https://rmf.org/wp-content/uploads/2018/05/Cloud_Computing_SRG_v1r3.pdf

on systems and code residing outside the system boundary, so long as the team who maintains the system inside the boundary are US persons.

Continuous Monitoring also requires ongoing bandwidth by qualified employees. The *FedRAMP Continuous Monitoring Strategy Guide*[9] includes a table of ongoing required operational activities which need to be staffed. Optionally, Continuous Monitoring can be outsourced to one or more managed service providers.

How much does our company know about FedRAMP?

This compliance framework is much more prescriptive than others you and your team may have encountered before. Each required control needs implementation, documentation, and monitoring. FedRAMP has a comparably daunting control count relative to other popular frameworks like SOC 2 and ISO 27001 as shown below.



Comparable control counts of popular cybersecurity frameworks

[9] https://www.fedramp.gov/assets/resources/documents/CSP_Continuous_Monitoring_Strategy_Guide.pdf

Of interest, *FedRAMP Tailored* is a relatively new program designed to accelerate time to market for low-risk SaaS applications. The FedRAMP Tailored policy page[10] includes qualifying questions you can review with your sponsor during the categorization of your system. Notably, the system cannot contain any personally identifiable information (PII) beyond the username, password and email address used to register users.

Early Preparation Priorities

Having a sponsoring agency is a significant milestone, and should be your primary objective after you decide to pursue federal business. If your team is new to NIST and FedRAMP, a workshop can help you come up to speed. An analysis of your opportunities can help you plot a path to fund iterations to your security program as you expand your products to a wider customer base.

Just setting up the pursuit of FedRAMP may take some time. Concurrent to this effort are several initiatives you can start right now that will accelerate your path to FedRAMP and strengthen your company in general.

Establish a Robust Security Program

Key to a robust security program, beyond technology considerations, is how security is practiced by the people in their everyday jobs—the culture. Take a hard look at the training, policies, procedures that are in place to protect your customers and your business reputation. Are they ready for the scrutiny of a federal audit? If your policies and procedures are acceptable, how well can you demonstrate that your people follow them? Is your security training tailored to the various employee roles (basic users, executives, tech workers, data owners, human resources, etc).

A security-first mindset across your organization will yield many benefits. When your employees can generally discuss NIST standards in the hallways, you will know they are naturally thinking about security aspects of their work.

[10] See https://tailored.fedramp.gov/policy/

Embrace Automation

Some companies build their production systems exclusively using your cloud provider's web console, manually. Managing multiple similarly-configured environments is slow, costly and error-prone without automation. It's also difficult to train new hires to support handcrafted cloud resources. It's especially difficult to explain to your auditors how your systems were built, and to demonstrate how you control changes.

> Investing in automation will make FedRAMP easier.
> We'd go so far as to say it's a prerequisite.

You need not "automate everything" to ready your product. FedRAMP benefits most from a few key foundational automation practices. Changes to cloud resources can still be triggered manually, but the build should be automated. Automating the build means you need to define your infrastructure as code. Infrastructure for each layer of your shared services and application workloads should be defined and built with code, preferably checked into a version control system for auditing purposes.

Cloud providers are making great strides in automating resources for FedRAMP systems. But beyond managing cloud infrastructure, automation is also great for managing the required compliance documentation. Its an exciting step that the GSA is developing a common machine-readable language[11] to accelerate documentation automation innovation.

Offload Compliance

The more services and processes you delegate to your underlying cloud provider, the less compliance management you are responsible for. Minimizing compliance scope is a crucial first step, and one of the best ways to minimize your cost and time to market. Setting scope involves more than drawing a tight box on a network diagram. Carefully scrutinize your labor costs. When reviewing the design of your platform, look for opportunities to replace do-it-yourself solutions with authorized managed services. For example, if you've been building container clusters from scratch, now is a good time to consider container services offered by your cloud provider. You can minimize the

[11] https://github.com/GSA/fedramp-automation

amount of underlying technology your team needs to manage and offload compliance burden.

> For lowest cost and fastest time to market, consider serverless options. Managing an operating system yourself comes with a host of required costly FedRAMP controls including image management, privileged user management, file integrity monitoring, anti-malware protection, backups, logging, and much more. Watch for more innovation in this space.

Conclusion

Successfully launching a new line of business for federal customers can be lucrative. FedRAMP is required for cloud services consumed by federal agencies. The system preparation, authorization process, and ongoing upkeep will require substantial effort, but for some companies the return justifies the investment.

To jumpstart your journey, you can take steps now to establish your information security management program and foundational automation practices. Now is also a good time to replace cumbersome self-managed parts of your stack with authorized services from your cloud provider.

> If the topics in this paper have covered any new ground for your team, our team can help you come up to speed and make the most of your opportunity. If the content here is old hat, we can accelerate your system build through establishment of best-practice automation fundamentals.

For more details on the FedRAMP authorization process, see the document published by FedRAMP: *CSP Authorization Playbook: Getting started with FedRAMP*, which covers these topics and more in depth. Learn more about FedRAMP at FedRAMP.gov.