FedRAMP

# FEDRAMP ACCELERATED

## A CASE STUDY FOR CHANGE WITHIN GOVERNMENT

## **REFLECTIONS FROM SPRING 2017**

# INTRODUCTION

The Federal Risk and Authorization Management Program (FedRAMP) began in 2011 as a way to ensure the security of cloud services used by the US Government. Federal Agencies needed a way to trust using cloud services, as they constantly cited security as a prime reason for not using those services. FedRAMP addressed that fear by using the government's existing security practices and operationalizing them for cloud environments.

However, four years into FedRAMP's existence, the security authorization process we created had ballooned from taking six months to complete to taking 12-24 months. The FedRAMP team knew we needed to change. With the evolving technological and cybersecurity landscape, the Federal Government needs to adopt cloud-based services while protecting its data. If FedRAMP continued to be too costly and time consuming for vendors, Agencies would no longer have a centralized process by which they could secure their data.

But any change would not be the "right" change unless we heard directly from our stakeholders to understand how our processes contributed to lengthy authorization timeframes. We reflected on feedback we collected and collaborated on ways to introduce efficiency while still maintaining the integrity of the FedRAMP program. We were ready to transform the program to make it faster and cheaper because if we didn't, we were at risk of alienating all of the stakeholders our program was designed to serve.

When we began the "FedRAMP Accelerated" initiative, the following conversation was the "Aha!" moment that gave us courage to transform :

*"What did you do before FedRAMP?"*
*"There wasn't anything before FedRAMP."*
*"If you created this process, then you can create a new process. The only thing stopping you is you."*

Many times within government, we are afraid to change a process or how we do our job simply because it is the way things have always been done or because of the inevitable, sometimes unwelcoming, reaction to change. We rejected this line of thinking outright and pushed forward under the proposition that a program built from scratch could be rebuilt - only better.

This is the story of how FedRAMP transformed itself within one year to reduce security authorization timelines from 12-24 months to a consistent timeline of less than six months to completion.

# TABLE OF CONTENTS

# BACKGROUND

FedRAMP is a government-wide program, established in 2011, that provides a framework for Federal Agencies to secure cloud services and products that comply with White House and National Institute of Standards and Technology (NIST) requirements. FedRAMP's primary objective is to provide a re-usable security authorization model by which Agencies can obtain safe, secure cloud service technologies to help modernize Federal IT.

There are two ways Cloud Service Providers (CSPs) can achieve a FedRAMP security authorization: by working with the FedRAMP Joint Authorization Board (JAB) and the Program Management Office (PMO), or by working directly with an Agency and having that authorization validated by the FedRAMP PMO. In meeting our primary objective, FedRAMP is focused on:

- Ensuring cloud services housing Federal information meet required Federal security standards
- Eliminating duplication and reducing costs
- Enabling the Federal Government to accelerate the adoption of cloud computing

The JAB is comprised of the Chief Information Officers (CIOs) from Department of Defense (DOD), Department of Homeland Security (DHS), and the General Services Administration (GSA). The FedRAMP PMO, housed in GSA, is responsible for facilitating and innovating the process and convening stakeholders

The requirement for the Federal Government to issue security authorizations for any IT system is based on the Federal Information Security Management Act (FISMA) and White House policy. Cloud providers that want to work with the Federal Government are required to follow NIST standards and requirements that cover all aspects of their system, from things like background investigation requirements of employees, to encryption of data, to physical security of IT assets.

# FEDRAMP'S FIRST FOUR YEARS

As FedRAMP evolved from an idea to a fully operational program, it followed the same patterns of development and maturity as most startups. After launch in 2011, we focused on developing the FedRAMP security requirements and core processes, establishing relationships with all of our stakeholders - CSPs, Third Party Assessment Organizations (3PAOs) and Federal Agencies - establishing a 3PAO accreditation program, and authorizing our first cloud systems through the JAB.

Over the course of the first two years, we established a rigorous baseline of requirements for securing the cloud that Agencies trusted and began to use. In 2014 and 2015, we focused on increasing Agency adoption of FedRAMP and cloud through scaling our JAB authorization process and engaging with Agencies to initiate authorizations at the Agency level. During this time we increased the number of FedRAMP-authorized cloud systems to more than 50, with over 150 individual Agency authorizations (an average re-use of three Agencies per system). We also placed a large emphasis on establishing an operational structure for continuously monitoring the security of authorized systems through the FedRAMP Continuous Monitoring (ConMon) requirements to validate that FedRAMP-authorized systems had the operational maturity to maintain low levels of risk within their environments.

One of the overarching goals for FedRAMP is to create a sustainable model that meets all of the needs of our stakeholders - rigorous security for our Federal Agencies, but also speedy and affordable authorizations for CSPs. By 2015, FedRAMP security authorizations through the JAB were beginning to hit some roadblocks and were taking longer than both industry and the FedRAMP teams could manage and justify. We knew something needed to change, and we needed to act quickly.

## WHAT WERE PEOPLE SAYING?

In the summer of 2015, we began a direct outreach effort to talk to CSPs, Agencies, and 3PAOs engaged with FedRAMP to understand what we needed to change. We wanted to hear from those who liked the program, those who didn't like the program, and those who were anywhere in the middle.

Some of the feedback was not easy to hear. We heard from our stakeholders that the JAB authorization process took too long; the rigorous reviews did not always add value to a system's security; stakeholders were not clear on program expectations, which often seemed to be a moving target; and there was uncertainty about how to successfully complete the process in a defined timeframe. Vendors felt that FedRAMP sometimes required a prohibitively high amount of resources and delayed or prevented them from doing business with

the Federal Government. This was especially true for smaller vendors.

But with the negatives, we also heard more positive feedback. We heard that the FedRAMP standards were some of the best international standards for cloud security. FedRAMP improved the security of cloud systems in a way that provided customers with the confidence they needed to begin adopting the latest cloud technologies. This re-confirmed that the FedRAMP security requirements, although sometimes challenging for providers to meet, were rigorous enough to protect the Federal Government's information.

## WHAT WERE PEOPLE EXPERIENCING?

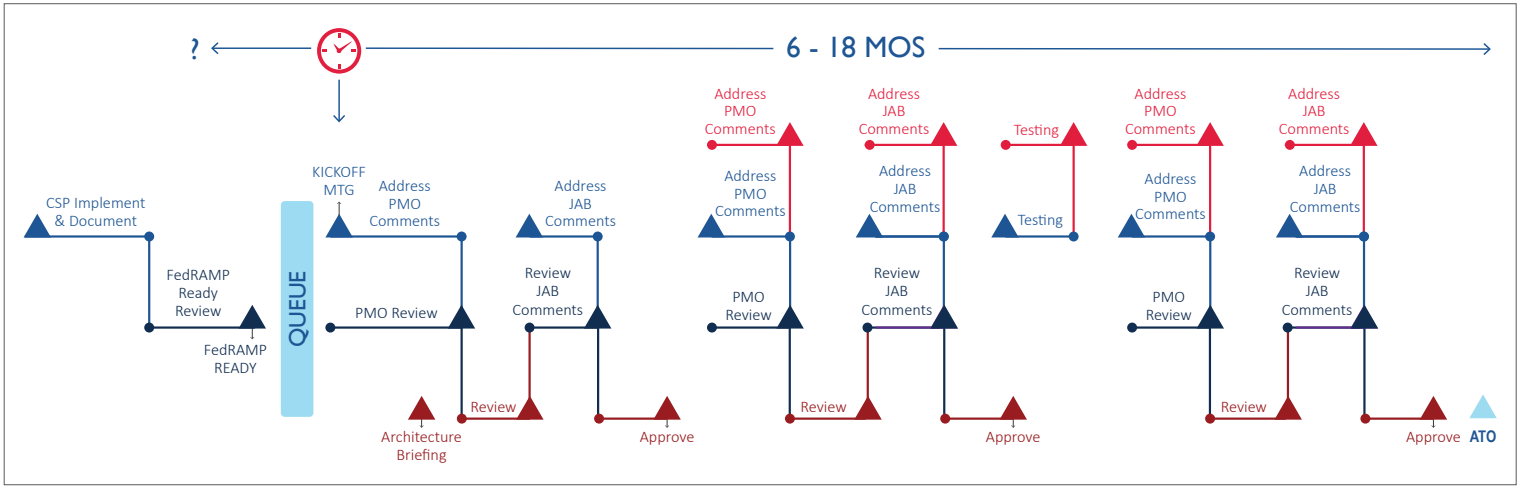
While all of this general feedback was incredibly valuable, it didn't leave us with anything actionable to do other than "speed it up" and "make the requirements more clear." We did not want to make quick fixes without knowing that we were going to make the right fixes and make the impact we wanted to our system as whole. In order to understand how we could change in a way that would be effective, we employed a design approach utilizing "customer journeys" to truly understand the FedRAMP experience from our stakeholders' perspectives. We brought in every type of stakeholder and mapped out their journeys with FedRAMP, from the first time someone said "Let's do FedRAMP," to the first submission of documentation to begin an authorization, to Continuous Monitoring post-authorization. We focused on mapping the JAB authorization process with our stakeholders because that is where we had the most control to transform and find the most efficient way to work with CSPs. We believed that if we could find the best path for the JAB, we could then share best practices with Agencies.

We utilized customer journeys through our design because we wanted to ensure we were thinking about how to solve the problems identified by our customers from their perspective. Our goal was to address the requests of our CSPs and 3PAOs and still meet the government's needs. The customer journeys were very detailed. We wanted to know every interaction our stakeholders had with FedRAMP - from CSPs to 3PAOs to our internal teams - and from their own unique perspectives. We wanted to know about every meeting, phone call, internal work, submissions to the PMO and JAB, reviews, etc. - basically anytime anyone even whispered the word FedRAMP. We wanted to understand not only the facts, but also the range of emotions our stakeholders felt because it impacted how they engage with FedRAMP and the overall brand and credibility of the program.

There were several interesting results from our journey maps. It was apparent that the PMO was not as responsive to our stakeholders as we needed to be. We realized we were not as transparent about the process as we thought we were. CSPs sometimes had internal conversations and strategy sessions with false assumptions about the process and requirements. Many times, we were not meeting the expectations of vendors or our internal teams by over-committing and relying on tools and processes that took too long, delivered little value, and did not provide the program with a high return on investment

relative to the level of effort. This led to our vendors and internal teams feeling frustrated and not seeing the light at the end of the tunnel for getting to an authorization.

After mapping out each stakeholder group's customer journey, we created a comprehensive view of the process for vendors to receive a FedRAMP authorization through the JAB (image below).




The comprehensive process mapping identified some glaring issues: the process was confusing; there were no clear decision points; there didn't appear to be anyone on first base making decisions; and there was a lot of duplicative work. A process that was created for rigor and security had become too complex to work efficiently and effectively.

## THE NEED TO CHANGE

While reviewing the feedback from both industry and our internal teams and analyzing our unified customer journey map, we knew we needed to address the authorization process if we were to continue to accelerate the government's adoption of cloud technologies. If we kept things the same, we would become yet another government program that stagnated and didn't change to address stakeholder input.

When we shared our findings with the JAB, they agreed on the PMO's recommended requirements for a redesigned process:

1) Authorization decisions in under six months
2) Same or less risk accepted by the JAB for authorizations
3) Equal or better quality of security authorization package documentation
4) Confidence that JAB resources were used efficiently, given limited capacity
5) Greater transparency and predictability in the process for CSPs, 3PAOs, and FedRAMP reviewers

Other than speed, all of the goals aligned with what had made FedRAMP's growth successful to date: solid risk assessments of CSPs, well documented system plans and assessment results, an effort to efficiently use team resources, and to be as transparent as possible. However, the first goal of the redesigned process was speed, which had never been a priority before. We had consistently said we wouldn't trade rigor for speed because security was the number one barrier to the adoption of cloud. However, now that we had three years of authorizations under our belt, it was time to see how we could incorporate speed into our overall goals while still maintaining our original goal of security first.

The FedRAMP management team took on the task of redesigning the authorization process through the initiative *"Accelerated."* Our goal was straightforward:

> We would transform the way we do security authorizations to ensure that we can make a decision to authorize or not authorize a system in less than six months.

While a simple goal, this wasn't a simple task. This pushed us to not only research and redesign the process, but prove the *Accelerated* FedRAMP process could work - and we did it all in less than a year.

# OPPORTUNITIES FOR CHANGE

Having commitment from the JAB on our five goals, we went to work. As we examined the authorization process, there were three key areas that stood out as the main problem areas: an overemphasis on documentation, only looking at security from a point in time, and duplicative work across members of the JAB and PMO. These were the three focus points for *Accelerated*.

## 1. SHIFT THE WAY WE UNDERSTAND A SYSTEM

The first step in our original authorization process was to understand a cloud system's capabilities through examining documentation. As a result, the emphasis of the security review was placed on the words in a document rather than true understanding of the capabilities of a system. The documentation reviews focused heavily on the CSP's System Security Plan (SSP) - which details all of the ~300 security requirements a vendor must meet. The SSP and attachment documents were often in excess of 1,000 pages of text. These reviews frequently took upwards of six months just to get to approval.

Documentation reviews would also many times lead to a contentious relationship between FedRAMP reviewers and CSPs because the reviews would "poke holes" in documentation until the language matched the requirement. This resulted many times in situations in which CSPs were providing language that didn't match what was actually implemented in a CSP's system, which would ultimately lead to risk findings during an assessment. Additionally, there were times when incorrect information was relayed by a CSP for a requirement in the documentation, which led to skepticism about the accuracy of everything else that was written in the documentation. Long story short, technical writing is hard and writing 500 pages of text describing a system almost always has some inaccuracies.

These document reviews wasted time and resources for both CSPs and FedRAMP because it rarely resulted in a complete and accurate understanding of the system or the risks associated with system use. We knew we needed to figure out a better way to understand the system other than through documentation.

## 2. "POINT IN TIME" AUTHORIZATIONS ARE NOT ACCURATE

In the original process, the only way that a vendor's ongoing security practices could be assessed was through a vendor's documented policies and procedures. There was no real ability for the JAB or 3PAOs to analyze a CSP's ability to maintain the security of their system through things like configuration management, vulnerability and patch management, active scanning, etc. Security assessments performed by 3PAOs were focused on a single point in time to see if requirements

were in place, but there was nothing in the process that focused on continued performance by CSPs throughout the authorization process.

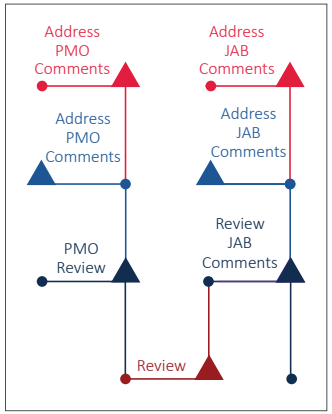
Using a "point in time" perspective, did not provide confidence that the CSP had the appropriate security processes in place to maintain their current security posture. When there wasn't a "good" picture of a system's security through the documentation, there was a lack of trust between FedRAMP and the CSPs.

To understand why this is a problem, we should reiterate that FedRAMP is not a certificate program. It is a risk management framework designed to authorize systems and continually ensure that a system is managing new risks and mitigating and fixing old risks in a timely manner. So by having a "point in time" authorization process both CSPs and FedRAMP were at a disadvantage. Ultimately, this meant that FedRAMP was getting a false picture of the security posture of a system .

Systems would get an authorization and then vendors would struggle to get back to the security posture they had at the time of authorization, and FedRAMP and Federal Agencies were using a system with more risk than originally authorized. We needed to create a way to have an ongoing view of a CSP's practices throughout the authorization process.

## 3. ELIMINATE DUPLICATIVE WORK

The final hurdle we needed to address was the most clear and direct pieces of feedback we heard from CSPs and 3PAOs: the FedRAMP PMO and the JAB review teams were performing duplicative reviews. For example, the PMO team would ask about the description of a security requirement, and then a JAB reviewer would ask a similar question but make a different request for how the CSP should describe it in their documentation. This added time and resources and did not provide for increased security of the system - just better documentation.




*One piece of the review process highlighted earlier is shown to the left to provide context to the duplicative reviews.*

The amount of duplicative work was a result of overlapping roles and responsibilities between the JAB and the PMO. This overlap was useful at the beginning of the program because it ensured that the JAB teams were only reviewing documentation that was "ready." However, these duplicative reviews ultimately created hurdles to speed and efficiency as the program scaled from five people and three systems, to 20 people and 30 systems. We needed to figure out a better delineation of work between the PMO and JAB teams to allow the teams to focus on their specific roles and responsibilities to make the process faster.

# RE-IMAGINING OUR PROCESSES

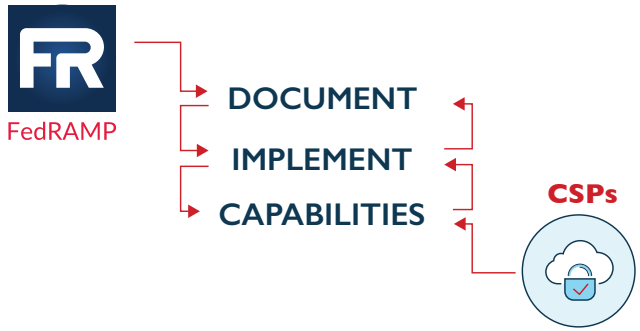
After we identified specific challenges of the authorization process that needed to be addressed, it was time to figure out how to solve them. Some of these problems were deeply rooted in the FedRAMP processes and in much of what Federal Agencies were doing across government.

The inspiration for our design process came from a scene from the popular movie about space exploration, *Apollo 13*. While this scene is a bit of hyperbole, it did inspire us to create a driving mantra: *"nothing's impossible, there's always a solution if you open your mind and think about the art of what is possible."* We knew we had all of the pieces for cloud security authorizations, but maybe there was a way we could re-use certain pieces, rearrange the way we do work, or more clearly set expectations and guidelines so that we could authorize systems faster than anyone in government has done before. We were committed to finding the right solution while keeping the same rigor of security that people have come to expect from FedRAMP and the JAB.

With our *Apollo 13* approach in mind, we homed in on those three key areas within the process that, if transformed, would have the potential for us to actualize our goals.

## FOCUS ON CAPABILITIES

The first phase of the security authorization process was by far the most time consuming. We first went to our customer journey maps to analyze this specific portion of the process. We put a CSP's journey and the FedRAMP team's journey side by side. Once we saw them next to each other, it became glaringly obvious we were approaching the authorization process from two totally different directions (see image below). FedRAMP began the process by analyzing documentation to understand a system's capabilities. CSPs began the process by implementing their capabilities and ended the process by documenting what they had in place.



In designing for *Accelerated*, we decided to embrace the CSP's customer journey instead of forcing industry to match how the government was doing work. In order to do that, we needed to figure out a way to perform a simple capabilities assessment up front to understand a CSP's system. That way a CSP and FedRAMP would know if a system had the right security in place to successfully complete the authorization process.

With the help of Agencies and industry, we created the FedRAMP readiness assessment. The FedRAMP readiness assessment would rely on the expertise of our FedRAMP-accredited 3PAOs and would operate more like a gap assessment that is performed by auditors in other industries. To keep the readiness assessment as manageable and low-cost as possible, 3PAOs would not need to gather evidence or address individual security controls. Instead 3PAOs would use their technical expertise to validate the capabilities of a system and provide the FedRAMP PMO with a simplified report attesting that the CSP has the necessary capabilities in place to achieve a JAB authorization.

Approaching the initial steps of the authorization from this direction helped us ensure that a system could adequately protect Federal information before embarking on the entire authorization process. Understanding the capabilities of the system first would make the entire process faster and build trust between FedRAMP and the CSP up front.

## INCORPORATE CONTINUOUS MONITORING INTO AUTHORIZATION PROCESS

At the outset, it was hard to believe that we were only looking at security from a single point in time. We were going through an 18-month process - how could we only be analyzing the system based on a single point in time? The customer journey maps clearly showed there was a lot of back and forth between FedRAMP and CSPs. However, even with the significant amount of communication during the process, the assessments and documentation were only conveying information about a system from one specific point in time. This problem was particularly troublesome knowing the speed with which many CSPs implement changes and new features on their systems.

In order to address this in our redesign, we decided to bring the ConMon program into the authorization phase, rather than beginning this post-authorization. ConMon requires CSPs to prove they are able to maintain the security of their system through a set of deliverables that provide visibility into the current system risks. These deliverables give insight into a vendor's processes around configuration management, vulnerability and patch management, and vulnerability scanning.

By incorporating ConMon into the authorization process, it bridges the gap between the "point in time" assessment and the need to understand how a CSP's processes worked in an ongoing manner. FedRAMP would be able to see how mature a vendor is in their business processes and their ability to run

their system in a secure way. This also would provide vendors insight into the rigor and level of effort required under FedRAMP's ConMon program earlier in the process. This would allow FedRAMP to only authorize vendors with mature processes to manage their system.

## CLEARLY DEFINE JAB AND PMO ROLES

Finally, we needed to think about how the JAB teams and the PMO worked together. The feedback and customer journeys showed a lack of clear delineation between the roles and responsibilities of the PMO and the JAB reviewers. A CSP would begin work with the PMO; the PMO would coordinate work between a CSP and the JAB; and ultimately the JAB would make an authorization decision. And since the ultimate decision maker in any authorization was the JAB, we needed to rethink how they were involved in the authorization process from the beginning.

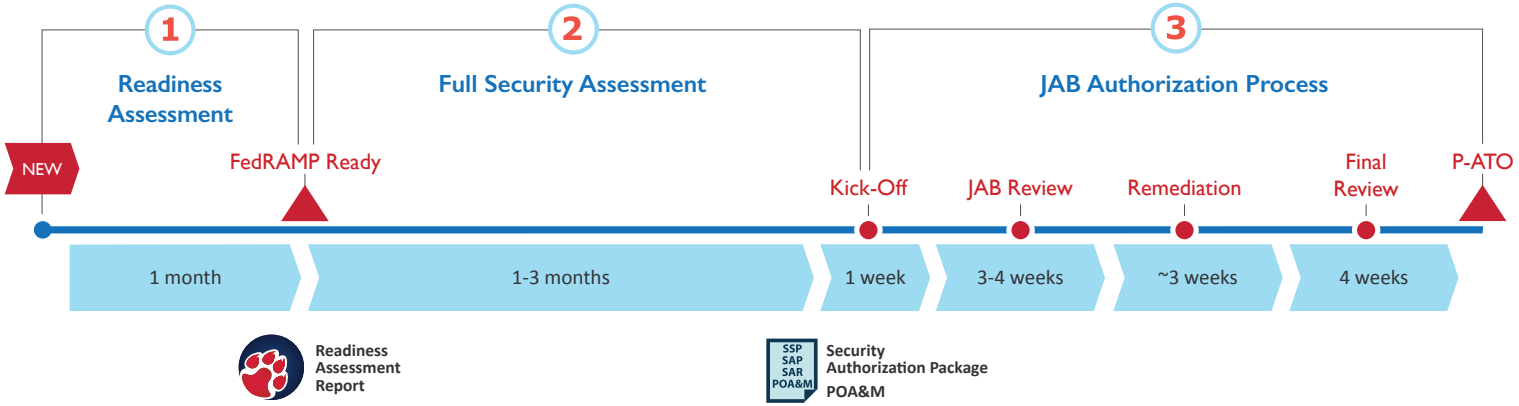
When FedRAMP started, the FedRAMP PMO and JAB teams created a formal JAB charter to define the roles and responsibilities of the PMO and JAB members. After three and half years, it was time to revisit that charter and determine how to most effectively work together. The JAB teams needed to engage with CSPs more directly without the PMO being the middleman. The new JAB Charter spelled out that:

- The PMO focuses on communicating expectations, providing the correct templates, answering CSP process questions, capturing the nuances of JAB requirements, ensuring the schedules and deadlines are met, and opening the channels of communications between the JAB and the CSP and 3PAO.
- The JAB reviewers are now exclusively focused on performing in-depth reviews of the CSP's system and ongoing communication with the CSP and 3PAO within the defined schedule for the ultimate recommendation to the JAB CIOs (DOD, DHS, and GSA) for an authorization decision.

# TRANSFORMING THE AUTHORIZATION PROCESS

Once we figured out how to address the three key areas for improvement, we were able to transform the authorization process by embracing what worked well in the past and changing what was not working well. By implementing a capabilities assessment up front, including ConMon into the authorization process, and redesigning how CSPs, the JAB, and the PMO teams work together, it became clear that our goal of consistent authorizations in under six months was not only achievable, but realistic.

The new authorization process would focus heavily on a vendor's readiness to begin prior to even committing to work towards an authorization. CSPs would also begin the authorization with a completed security assessment. And the authorization process would have better defined roles and responsibilities with clear go/no-go decision points for moving through each phase.



The redesigned JAB authorization process has four key steps:

1) a Readiness Assessment,
2) FedRAMP Ready Determination,
3) a Security Assessment, and
4) the JAB Authorization Process.

## READINESS ASSESSMENT

The FedRAMP Readiness Assessment is the most fundamental change in the authorization process and makes it possible to complete an assessment in less than six months. This assessment ensures a CSP has prepared its system with the right capabilities prior to beginning an authorization. To put it into another context, no one would ever run a marathon without spending serious time training, because even though you might be able to finish 26.2 miles, it would likely take days instead of the average of about 4.5 hours. That's the same with the readiness assessment - it ensures that a vendor has done the right preparation in order to complete a FedRAMP authorization within an expected normal range of time.

## FEDRAMP READY DETERMINATION

Once a Readiness Assessment Report is provided to the PMO, the PMO determines whether or not a vendor is truly FedRAMP "Ready." The PMO works with the CSP and 3PAO to review the report and understand a CSPs technical capabilities. If a vendor achieves FedRAMP Ready, it is eligible to keep the status for up to a year.

## FULL SECURITY ASSESSMENT

The JAB requires a CSP to complete a full security assessment prior to kicking off for an authorization. Fulfilling this requirement means that the security authorization process will include all elements of the security authorization at the beginning of the review. This includes the SSP, Security Assessment Plan (SAP), and Security Assessment Results (SAR). This allows the review process to look at the system from a more holistic perspective instead of doing the review piecemeal.

The security assessment is both the responsibility of the CSP and the 3PAO and results in the full security authorization package. When a CSP and 3PAO are scheduling testing, they need to consider FedRAMP's Timeliness and Accuracy of Testing document, which outlines the timeframes of acceptable assessment evidence for new systems and those systems with existing Agency authorizations. The intent of this document is to ensure that CSPs don't go through a full assessment too early, which would result in assessment evidence that is too old and require a new assessment.

## JAB AUTHORIZATION PROCESS

The JAB Authorization Process is time-bounded and includes four key steps. Within each step, the explicit timeframes and decision points provide FedRAMP and CSPs with clear expectations of the process and creates better defined yes or no decisions so that we can mark forward progress within the authorization process.

The four steps in the JAB Authorization Process are:

1) **Kick-Off (one week):** This is a series of in-depth, face-to-face, collaborative sessions between the CSP, the 3PAO, the JAB, and the PMO to holistically review the system's capabilities, boundary and services, and any risks identified by the 3PAO during the full security assessment.
2) **JAB Review (three to four weeks):** This is an in-depth review of all of the security package documents by the JAB reviewers to note any risks, deficiencies, or areas needing more clarification.
3) **Remediation (estimated three weeks, no longer than 12 weeks, CSP dependent):** This is a dedicated time for the CSP and 3PAO to update system functionality, testing, and/or documentation based on the JAB comments during their review.
4) **Final Review and Approval (four weeks):** The JAB reviews the CSP and 3PAO remediation work to ensure all of their comments are addressed and provides their final approval for the CSP's provisional authorization.

Instead of working in a waterfall approach, the new process employs a more agile, iterative approach that allows for drastically decreased time to review a CSP's capabilities and security. Additionally, check out our more detailed guidance on the roles and responsibilities of 3PAOs and CSPs in the authorization process.

# TESTING FEDRAMP *ACCELERATED*

## (HINT: IT WORKED)

As we completed the design of this process, we tested it with three vendors to ensure that it worked. We wanted to evaluate in real time whether our redesign would translate from paper and minds to reality in FedRAMP's technically and socially complex landscape. We worked with the JAB to find three vendors of different sizes (start-up, mid-size, and large) and complexity (SaaS, PaaS, IaaS) to work with on testing out the process.

After vetting our three CSPs through the new process, we were able to get to an authorization decision within less than 20 weeks for each CSP[1]. Some key reasons why it worked:

### FEDRAMP READY

- Our three vendors worked through the first iteration of the readiness assessment and helped us refine expectations and the information needed to make this step successful. The vendors also expressed that the readiness assessment helped them align their expectations to better understand the requirements prior to beginning a full security assessment.
- With the lessened scope of review and a simplified report, the reviews of a FedRAMP readiness assessment could be completed within one week of submission. 3PAOs submitted Readiness Assessment Reports only if a vendor was truly FedRAMP Ready. This helped ensure not only that FedRAMP's resources are used wisely but also that our vendors were working collaboratively prior to engaging with the PMO and FedRAMP.

### FULL SECURITY ASSESSMENT

- Completing the readiness assessment prior to the full security assessment helped to eliminate a majority of the risk associated with completing a full assessment prior to kick-off. The readiness assessment incorporated all of the key areas that need to be identified and agreed to by the government and CSP prior to doing a full assessment - understanding a CSP's boundary, the services being authorized, and the core capabilities required for an authorization.
- The JAB was then able to receive the full documentation and testing from the CSP and 3PAO at the beginning of the

1 The three authorization decisions were made in 13, 16, and 20 weeks.

authorization process. This allowed them to have a baseline of trust that the system had what it needed to be secure. Therefore, the documentation review was a matter of clarification and providing additional necessary details.

## JAB AUTHORIZATION PROCESS

- The lengthened and enhanced kick-off meeting provided a much more holistic view of the CSP and risks from the beginning, which, according to the JAB reviewers, "saved what would have been a month in the old process."
- The updated JAB Charter ensured that resources were aligned correctly in order to make clear decisions throughout the authorization process more quickly.
- A steady communication cadence between the CSP and FedRAMP PMO (e.g., two conference calls per week) ensured information was exchanged quickly and accurately.
- An agile review process allowed the 3PAO and CSP to begin remediation activities while the JAB completed the balance of the review. For this to be done successfully in the future, the process will benefit from having dedicated reviewers to maintain scheduled milestones and expedite the process.

# LOOKING FORWARD: *WHAT'S NEXT*

Looking forward, we consider FedRAMP *Accelerated* to be complete. It was an initiative that is now operational - FedRAMP *Accelerated* is now the JAB authorization process. We are committed that all authorizations with the JAB will have a decision made within six months of beginning the process. Less than 18 months after testing this process, our authorizations have ranged from 12-19 weeks.

Additionally, we recently released our Agency Authorization Playbook - which takes all of our lessons learned over the past 18 months and puts it into an actionable guide for Agencies to complete authorizations in the same timeframes. We hope this can serve as a model for security authorizations that scales effectively beyond just those that are done with the JAB. It provides more opportunities for CSPs to participate in the Federal space securely and obtain a FedRAMP authorization in as speedy a manner as possible.

Finally, we've changed the process for selecting which vendors work with the JAB. We've begun a program called FedRAMP *Connect* where we publicly prioritize vendors for working with the JAB through a collaboration with the CIO Council and The White House.