Positioning for Federal Cloud Business

Posted At : June 24, 2014 5:19 PM | Posted By : Kyra Fussell

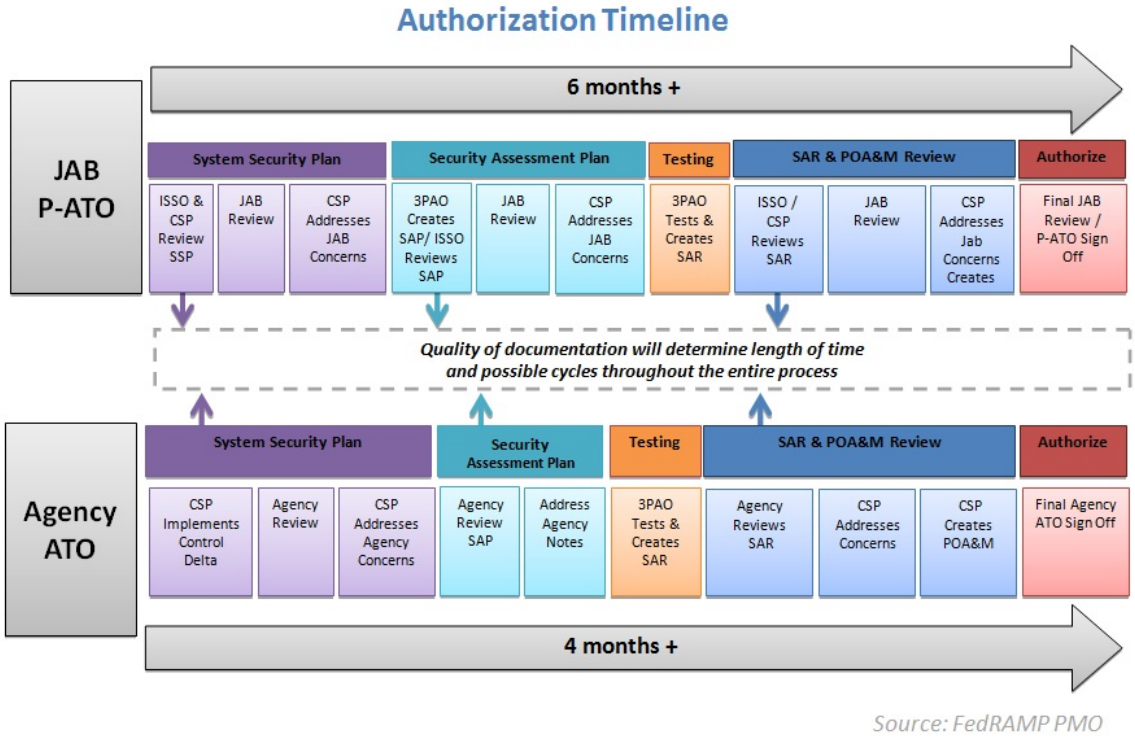
Related Categories: Digital Government, Information Security, Cloud Computing, Federal, General Services Administration (GSA)

The Office of Management and Budget (OMB) set June 5, 2014 as a deadline for cloud vendors to comply with federal cloud security certification. This mandate for federal systems highlights a debate that started in the vendor community as soon as the Federal Risk and Authorization Management Program (FedRAMP) outlined its process two years ago: Cloud providers have a few paths available to achieve compliance, some aspects of the processes depend on which route a provider takes. So, which one is best?

Whether they are commercial or government entities, cloud service providers have a number of responsibilities. They're responsible for working with a third party assessment organization to conduct initial and annual assessments. Along with maintaining an authorization (once granted), they must comply with continuous monitoring requirements. And above all, they are responsible for ensuring their cloud offering or service implements the FedRAMP security controls.

There are three paths for cloud service providers (CSPs) to become FedRAMP compliant. The first is to submit documentation to the FedRAMP program management office (PMO) for review by the Joint Authorization Board. The second path is to submit documentation to the FedRAMP PMO and review by an agency for Authorization to Operate (ATO). If a vendor receives ATO from one agency, the FedRAMP process will enable other agencies to use that service faster by decreasing the time for approvals. Finally, the third path is for a vendor to submit their documentation to the FedRAMP PMO. This "CSP supplied" path also shortens time for approvals because documentation and testing are prepared and in order for agency review. Ultimately, the difference between these categories is the level of review. JAB provisional authorization relies on review by the FedRAMP Information System Security Officer (ISSO) and JAB. Vendor offerings working toward Agency ATO will receive agency review. CSP supplied offerings have not yet been reviewed.

While there are several paths to compliance, there are only two types of cloud security authorization. One is awarded by the Joint Authorization Board (JAB), which is comprised of security experts from the Defense Department, Department of Homeland Security, and General Services Administration (GSA). The other type is agency sponsored. One difference between these two processes is the timeframe for each. (Obviously, the scale and complexity of the offering being evaluated also comes into play.) The FedRAMP PMO has estimated the time for each path to authorization, pending CSP readiness and responsiveness at each stage.



Source: FedRAMP PMO

It takes the JAB approximately 6 months to complete the process to award a Provisional Authorization to Operate (P-ATO). The JAB path focuses on government-wide offerings. At the same time, the JAB is unable to accept risks on behalf of an agency, which is why the authorization is provisional. If an agency decides to use a solution that's received P-ATO, the agency will need to issue its own ATO letter saying they accept the risk associated with the system. If a provider is working directly with an agency to establish ATO, the process can take around 4 months. Agencies are likely to target capabilities that align with their mission areas, technology strategies, and pain points. Since these vary from one agency to the next, an agencies stamp of approval might draw mixed interest from other organizations.

A provider who undertakes the process independently can complete the Security Assessment Framework in around 6 weeks. This faster timeline may sound compelling, but there is a catch. At the end of the process, the provider may be a candidate for authorization, but they have yet to undergo review by either the JAB or an agency. This CSP supplied option could be the perfect way for providers of specialized offerings to raise agency awareness. That attention comes at the expense of resources without the guarantee of any business.

Providers that are evaluating options for pursuing FedRAMP certification should also be aware of the program's recently updated security controls. The vendor transition plan to the updated FedRAMP baseline was released in April 2014. This plan divides cloud service providers into three categories based on their status in the FedRAMP application process. Providers that have reached the in-process stage or that are already in the continuous monitoring stage will have to comply with the new baseline during annual assessment. Their documentation and supporting elements must be updated using the new FedRAMP templates. Annual assessments will test around 140 or 150 controls including both the core ones and new additions. Also, the change of controls will be assessed due to system changes.

---

*Originally published in the **GovWin FIA** Analysts Perspectives Blog. Follow me on Twitter **@FIAGovWin**.*