

servicenow[™]

FedRAMP Paves the Way for Cloud Adoption



FedRAMP Paves the Way for Cloud Adoption

Just as many industries have turned to cloud computing, the federal government has started adopting cloud for efficiencies and cost savings. Agencies in the vast federal government also see another benefit: a way to standardize a huge mix of IT systems.

Federal agencies are under continuing pressure to update their IT systems with the latest technology and ensure they're run at the highest level of safety and security. For decades, that's meant continued software and hardware updates, and then painstaking integration of those new or updated systems into existing infrastructure. In the past, nearly every agency had its own stack of systems that needed to be maintained in large data centers.

Now, agencies increasingly are partnering with commercial cloud infrastructure providers. With cloud, such upgrades and integration can be easier and faster. There are also cost savings associated with needing fewer IT professionals because information is stored remotely, rather than on local servers.

There have been challenges to this transition. The Federal Risk and Authorization Management Program (FedRAMP) was introduced to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based products and services.

Prior to FedRAMP, a company wanting to sell cloud-based products to two or more federal agencies had to go through separate approval processes. FedRAMP standardizes access and control features across all agencies, eliminates redundant security assessments done by different entities, and is more cost-effective for the government's overall tech activities.

Compliance with FedRAMP is mandatory for all agencies, with a few exceptions, and commercial suppliers must be in compliance with the program. Demand is growing. To date, more than 100 agencies are using FedRAMP-authorized products.¹ Cloud service providers are addressing the cost and compliance issues raised by FedRAMP.

According to Bloomberg Government, the market for federal cloud services has grown an estimated fivefold since 2010, from about \$1.3 billion to a projected \$6.5 billion in fiscal 2018.² Although it is not easy to get FedRAMP certification, it can be used across the government once attained.



The market for federal cloud services has grown an estimated fivefold since 2010.

¹ FedRAMP, <https://marketplace.fedramp.gov/#/agencies?sort=name>

² Chris Cornillie, "Three Takeaways from Trump's 'Cloud Smart' Strategy," *Bloomberg Government*, Oct. 2, 2018, <https://about.bgov.com/blog/three-takeaways-trumps-cloud-smart-strategy/>

Cost Exceeds Estimates

One of the biggest benefits of cloud is that it can simplify updates and fixes. Without cloud, agencies would have to install a system on every computer in the federal government. Using cloud should increase efficiency when addressing security breaches and updating software to the latest versions. Agencies don't need a specialist in each system, whether that's a word processing program, graphics software, or something else. Each agency can feed off the same version on the cloud. If there's a problem, consultants or specialists can solve it across agencies without having to be paid by a specific agency.

But while the efficiencies and cost savings make sense over the long term, initial adoption has been more expensive than initially anticipated. That's been the case for both government agencies and private vendors.

"There's a lot of scale to cloud, and initially they thought the cost was going to be much less," said Katie Lewin, federal director of the Cloud Security Alliance and former director of the federal cloud computing program.

For one thing, various agencies still need to upgrade existing infrastructure. Using vendors doesn't mean agencies don't need to do anything to their networks. A 2018 survey³ by MeriTalk found 67 percent of government agencies' legacy network infrastructures not ready to handle cloud migration or cloud and hybrid networks. About half of managers said the biggest holdup has been lack of prioritization to update networks for cloud adoption.

To get there, managers said networks would have to increase capacity and speed and reduce complexity. By modernizing the network, agencies can reduce the time needed to migrate to the cloud and ensure cloud strategies reach their full potential.

Some agencies are further along than others in the process. Some are early adopters, while others struggle to learn and integrate the new technologies, and don't have the right expertise.

"Getting your data integrated and connected is also a major issue. There is a significant outlay of getting your data onto the cloud," said Kevin C. Desouza, professor of business, technology, and strategy at QUT Business School, Queensland University of Technology in Australia and a nonresident senior fellow at the Brookings Institution.

"Agencies that have effective data governance practices in place are going to find it easier. In addition, agencies that have a propensity for, and experience with, adopting and implementing emerging technologies will find it better," Desouza said.

Given the complexity of the project, some agencies have found it necessary to set up a digital transformation office staffed with experts to shepherd projects and train existing staff. Some examples include the General Services Administration's 18F, the Treasury's Treasury Digital Service, and the Defense Digital Service at the Department of Defense.



Some are early adopters, while others struggle to learn and integrate new technologies.

³ MeriTalk, "Cloud Complexity: Navigating the Network Piece of the Federal Cloud Puzzle," Oct. 15, 2018, <https://www.meritalk.com/study/cloud-complexity/?campaign=pressrelease>

"You have to train employees on new systems and processes, and that takes time and money," said Darrell West, author of many books on how technology transforms the way we work and founding director of the Center for Technology Innovation at the Brookings Institution. "For some people, it is hard to adjust to new ways of doing things."

Requirements for Vendors

For vendors looking to work with the government, many extra steps are needed to attain FedRAMP certification. At the most basic level, companies need to have a systems security plan.

"If you don't have basic stuff like a security plan and a couple other documents, then you have no business applying for FedRAMP because you don't have the documentation needed to support it," Lewin said. The FedRAMP site has many resources, she said, to help companies through the process.

Vendors also need to be prepared for other requirements. For instance, one issue that came up when agencies started adopting cloud was the geographical location of the grid. Corporations using cloud might find their data is scattered all over the globe—which could be deemed a security risk to government agencies.

"The federal government doesn't want their data going all over the world," Lewin said, "so one of the accommodations that cloud service providers have is they have U.S.-only clouds, which I think makes everyone feel more comfortable."

Another issue is ownership of data. The cloud service provider needs to establish that the government owns the data in the cloud. All these additional requirements are extra costs for companies looking to work with the federal government.

Improvements to the FedRAMP Process

FedRAMP was introduced in 2011 soon after Vivek Kundra, then the federal chief information officer, came out with a "Cloud First" policy, which encouraged agencies to use cloud computing as a faster, safer, cheaper way to maintain and deliver data inside the agencies, to other agencies, and to the public.

FedRAMP actually whittled down a set of controls set by the Federal Information Security Management Act, applying only a subset of relevant controls for agencies to follow. Agencies decided what products they wanted to use and then were expected to conduct a review to get the "authority to operate." That process got complicated, so the Joint Authorization Board was created, comprising chief information officers from the GSA, Department of Defense, and Department of Homeland Security.

Creating these standards and coming up with this process has helped both the federal government and vendors save money. FedRAMP is estimated to have helped the government avoid \$178 million in costs over six years.⁴



FedRAMP has helped both the federal government and vendors save money.

⁴ Meritalk, "GSA Offers Guidance on Moving to Cloud With FedRAMP," July 23, 2018, <https://www.meritalk.com/articles/gsa-offers-guidance-on-moving-to-cloud-with-fedramp/>

To speed up the process, agencies can now share an authority to operate, or ATO. So, for instance, if one agency has a case management system that got an ATO, another agency can use that same ATO based on the work that was done already.

"It is just starting to happen now, this idea of cross-agency acceptance so everybody doesn't have to start from scratch," Lewin said.

In March 2018, the GSA said it tried an accelerated FedRAMP process with three vendors, successfully reducing the time to authorization to about three months, down from a year. That process is now the norm and there is a possibility that could be further reduced after the Government Accountability Office conducts its audit.⁵ The audit will review the 24 major federal agencies' use of FedRAMP, as well as vendors' experience in the whole process. The audit could also push agencies to expand their use of cloud computing services.

To further accelerate the process, FedRAMP has introduced different classifications for approval. For instance, FedRAMP Tailored reduces the number of security requirements to 35 from 125 for low-risk use cases such as cloud collaboration tools, project management applications, or other software-as-a-service systems.⁶ FedRAMP also started a program called FedRAMP Connect, which puts some vendors on a priority list to work with the Joint Authorization Board, based on demand from government agencies.

"This is slowly churning," Lewin said. "Setting up something in the government, or anywhere really, is really hard. But lots of companies have investments now, they've gone through this process, so that's already a cost to them. I think that it is now pretty well established."

⁵ FedRAMP, "How FedRAMP Transformed JAB Authorizations to take 75% Less Time," March 28, 2018, <https://www.fedramp.gov/how-fedramp-transformed-jab-authorizations-to-take-less-time/>

⁶ Meritalk, "GSA Offers Guidance on Moving to Cloud With FedRAMP"



About ServiceNow

ServiceNow (NYSE: NOW) makes work, work better for people. Our cloud-based platform and solutions deliver digital experiences that help people do their best work.

For more information, visit: www.servicenow.com.