Making the Most of FedRAMP

Industry Perspective

cisco | verizon

Executive Summary

When the Federal Risk and Authorization Management Program (FedRAMP) launched in 2012, cloud computing was a fairly new business model in government. Few agencies were buying IT services and they were struggling to grasp the logistics of cloud procurement, implementation and security.

Fast-forward to the present. Virtually every Cabinet-level agency, including the Defense Department, is investing in cloud. FedRAMP has played a key role in that adoption by establishing a common baseline for securing cloud products and services.

Despite the progress, "it's important for agencies to realize that we're still in the beginning phase of FedRAMP maturity," said Daniel Kent, Senior Director and Chief Technology Officer of Cisco's U.S. Public Sector Organization. "There are about 16,000 cloud applications out there today, and only about 70 have been authorized by FedRAMP."

But agencies at all levels of government see the value in using standards to improve cloud security. Although FedRAMP is a mandatory federal program, there is a growing number of state and local governments using the same requirements to evaluate their cloud service providers. The benefits include time and cost savings when verifying security practices at those companies, as well as a level of assurance that vendors have met rigorous security requirements. "FedRAMP has become a seal of approval with expanded value beyond the federal market," Kent said.

To help government make the most of FedRAMP, GovLoop partnered with Cisco, a market leader in networking tools and FedRAMP-authorized cloud provider, to produce this report.

To glean from Cisco's insights GovLoop sat down with Kent and Andy Campbell, Business Development Manager of Cisco's U.S. Public Sector, Regulated Cloud, to help agencies better understand what FedRAMP entails, how it can help them and practical tips to get the most out of the program.

The Federal Risk Authorization Management Program (FedRAMP) is a government wide program that provides a standardized approach for assessing the security of cloud products and services, authorizing them for government use and continuously monitoring the long-term security of those cloud solutions.

FedRAMP

The Value of FedRAMP

Although there are federal standards that govern security of IT systems, cloud is a new way of doing business for many agencies. It enables them to buy hardware and software as a service, rather than acquiring those assets on their own.

But depending on the agency, cloud vendors were often forced to meet varying security requirements for the same cloud product or service. This process was not only costly for the vendors but also for agencies. They were spending an exorbitant amount of time and money to conduct lengthy security assessments and authorizations for the same cloud services.

What FedRAMP did was establish standard security requirements for cloud vendors. By taking the guesswork out of cloud security, FedRAMP has helped move cloud adoption forward.

Here's how:

FedRAMP's approach uses a "do once, use many times" framework that saves an estimated 30 to 40 percent of government costs.

As of October 2016, 77 cloud solutions were authorized through FedRAMP, and an additional 49 products and services were under review.

More than 34 agencies attended FedRAMP's first agency roundtable in September. The goal was to build connections and share cloud security and implementation strategies across government.

Not only did FedRAMP establish requirements for securing low- and moderate-impact systems, but in June 2016 the program rolled out requirements for securing high-impact systems in the cloud. Each impact level defines the severity of damages to an agency if the system's operations were disrupted in any way.

High-impact systems are those that are necessary to support agencies' continuity of operations. Both industry and government have been working through the growing pains of speeding up the FedRAMP process and addressing lingering security concerns.

To better understand agencies' needs and support their cloud journey, the program brought on Ashley Mahan, its first Agency Evangelist. Her goal is to help agencies embrace FedRAMP and ultimately adopt secure cloud services.

"Some agencies are still trying to understand how FedRAMP will help them, and we offer more services than just the authorization," Mahan said in an interview with GovLoop. Those services include trainings, webcasts, events and templates to help agencies take advantage of all FedRAMP has to offer.

"As stakeholders better understand the services we can provide, they will know that they can come to us for more support," she said.

Three Key Agency Takeaways About FedRAMP

There are three things that agencies should keep in mind as they navigate the ins and outs of FedRAMP, said Campbell:

Data Sovereignty

Data sovereignty, or the concept that information converted and stored in binary, digital form is subject to the laws of the country where it's located. There aren't FedRAMP requirements that data must reside in the U.S., but the program details multiple security controls about where data is stored, what the boundary of the system is and where and how data in transit is protected. Each agency is responsible for putting restrictions on data location, if needed.

Data Security

Data security is foundational to FedRAMP. The program's requirements are derived from National Institute of Standards and Technology (NIST) security controls. But FedRAMP includes additional security requirements above what's detailed in NIST SP 800-53 rev4, which outlines standards for securing low- and moderate-impact government systems. The publication includes rules and controls for accessing systems, incident response, continuity of operations, disaster recovery and more.

Data Access Control

Data access control, or how organizations monitor and manage who has access to cloud systems and how quickly they can detect and mitigate unauthorized access to those systems. FedRAMP addresses user access requirements, but the agency is responsible for managing who has what privileges within the system and for disabling accounts when employees no longer need access to a system. In the next section, we'll explore the types of secure cloud services agencies can buy under FedRAMP and how Cisco fits into that growing ecosystem.

The Evolution of FedRAMP Cloud Services

The diversity of FedRAMP-authorized products and services has grown drastically since the program launched in 2012.

As of October 2016, more than 70 cloud services were authorized for government use under FedRAMP, with another 49 services in the process of being authorized. Those offerings cover a range of deployment models — dedicated government community clouds, as well as hybrid, private and public clouds — and different service models, which include infrastructure, software and platform as-a-service.

A quick glance at the FedRAMP dashboard shows that the number of authorized cloud service providers has more than doubled and includes both private companies and government entities that offer cloud services to fellow agencies.

In the early stages of cloud adoption, agencies were mostly consumers of infrastructure-as-a-service (IaaS). In IaaS models, the cloud provider manages the underlying infrastructure, while the agency controls the operating system, storage, applications and select networking components, such as firewalls. But as adoption has matured, agencies are increasing their use of software services, an area where Cisco sees great promise for agencies in terms of savings and increased work productivity. "Cisco has a large installation base of collaboration solutions in the federal market, but that number largely consists of on-premise collaboration tools, such as phone and video conferencing systems," Kent said. "They are typically owned and operated by the government on their own premises. But as we move to the next generation of collaboration, agencies are migrating to cloud-based applications and collaboration systems."

As agencies' needs change to support a diverse workforce or remote employees, Cisco is providing the tools and capabilities to meet those needs. For example, Cisco worked directly with the Health and Human Services Department to certify that its Webex® Web Conferencing platform met FedRAMP standards.

Cisco is currently working with HHS to also approve its hosted collaboration solution for government, which includes voice, video, instant messaging and presence. A FedRAMP authorization is expected by the end of 2016.

"When we put the hosted collaboration solution for government together with Webex, we will have an extremely robust and broad set of services related to unified communications for our customers to take advantage of," Campbell said. "We provide the same functionality, capabilities and experience that commercial customers are accustomed to, and now all of that is available through a FedRAMP-authorized service."

How to Take Advantage of FedRAMP

FedRAMP is about more than standardizing cloud security across government. One of the biggest benefits it provides is the ability for agencies to reuse and build on one another's work.

Rather than each agency re-evaluating the same cloud services, they can share notes and ask questions to determine if those services meet their needs. The premise of FedRAMP is that the baseline standards it provides cover requirements that are common across agencies. That frees agencies up to focus on the few requirements that may be unique to them.

"Individual agencies can accept their own level of risk associated with a cloud service when authorizing that cloud service (as allowed by the Federal Information Security Management Act), [but] one agency may be hesitant to reuse another agency's authorized cloud solution because it may not trust the risk tolerance associated with that authorized cloud solution," Mahan told GovLoop.

To help ease these concerns, she said that FedRAMP is supporting agencies to:

Provide high-level education about, the cloud security and the FedRAMP program.

Standardize the documentation and review process. FedRAMP encourages agencies to perform their due diligence in reviewing all security documentation that is located within the FedRAMP secure repository prior to issuing an authorization.

Clarify the risks that the authorizing agency accepted. FedRAMP is applying safeguards to ensure agencies are well informed prior to reusing an agency-sponsored Authority to Operate (ATO). The FedRAMP team reviews each sponsored agency standard ATO package and provides a summary report (three to four pages) outlining the system risk to ensure each agency makes an informed review and decision. FedRAMP retains a copy of all authorized cloud service providers' security documentation and assists agencies in performing their due diligence in reviewing all security documentation.

Agencies have been shouldering more of the responsibilities of working directly with cloud providers to complete the authorization process. Initially, the FedRAMP Joint Authorization Board (JAB), the program's primary decision-making body, had that task.

"From the beginning, we've always said the vast majority of authorizations should go through agencies," FedRAMP Director Matt Goodrich said at a government cloud computing conference. "They should not be going through the Joint Authorization Board. The Joint Authorization Board has limited funding. When we launched FedRAMP, every agency said, 'We don't want the department of FedRAMP. We don't want everything to go through one centralized placed. We still want some control over the IT that we manage and that we buy and use.'"

But products and services used broadly government wide are ideal candidates for the JAB.

Federal agencies can review FedRAMP authorization packages through the secured document repository on the OMB Max website. State employees are not allowed to review FedRAMP security documentation, but they are encouraged to contact any FedRAMP-authorized provider directly to learn about their security package specifications.

The best approach for government is to engage vendors early in the process when they're considering moving to the cloud, so that they understand what's included and excluded from the FedRAMP security package. This documentation outlines how a company's security practices align with FedRAMP requirements.

When reviewing the package, agencies should consider whether the security controls outlined meet agency requirements. Other tips from FedRAMP.gov include focusing on whether the agency that did the initial authorization is using the system in the same manner as your agency and if the data being stored in the cloud requires the same level of security.

"Before you ever get to the procurement cycle, it's good to review the FedRAMP package and then come to the cloud service provider with your questions and ask for clarification or for more detail," Campbell said.

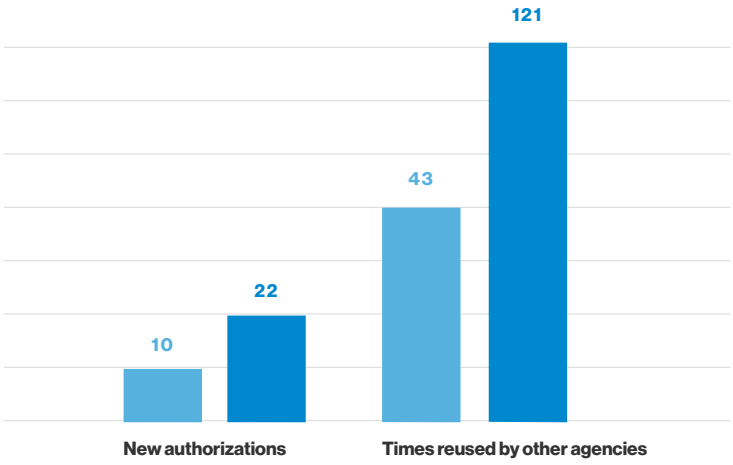
Some agencies have waited until the procurement phase to ask questions and divulge their terms and conditions for data security that vendors are expected to follow. Delaying these discussions creates unnecessary burdens and setbacks for the agency.

To prevent these issues, agencies need to have the right people at the table to review a cloud provider's security plan and ask any pertinent questions early on.

Campbell suggests including the agency's security team, particularly the chief information security officer and chief information officer, who ultimately authorize that a cloud service is OK for use within the agency, as well as procurement officials and your agency's general counsel. Working with prospective cloud vendors early in the decision making process and assembling the right team will ensure your agency invests in the services that best meet its needs.

Here are a few stats that show how reuse of FedRAMP authorizations has increased government wide:

FedRAMP agency authorizations



Fiscal Years: 2013–2014 and 2015–2016

In 2015, FedRAMP noted that agencies avoided $70 million a year in costs because they no longer had to start from scratch and re-evaluate cloud providers on their own.

Cisco's Approach to Data Security

Campbell highlighted some of the key areas that Cisco addresses when it comes to cloud security:

Dedicated Deployments

Cisco has a governance model for ensuring that only government entities and U.S. persons have access to cloud systems, the underlying infrastructure and data stored in those systems.

End-to-end Encryption

The company offers FIPS 140-2 compliant encryption for all data. The cloud system is continuously monitored, 24 hours a day, seven days a week, and scanned for any globally known security vulnerabilities, unauthorized access or changes to the system. Staff are trained to identify, remediate and notify customers if anomalous activity is identified.

Policy Enforcement & Management System

This robust system ensures that anyone who has authorized access to the system — either at Cisco or a customer agency — is performing only the tasks they are permitted to do.

FedRAMP is the Future

As required by FedRAMP, cloud service providers are constantly under review and subject to regularly scheduled audits to ensure that they maintain their FedRAMP authorization. Although cloud providers have a huge responsibility to keep systems secure, agencies still own the data and must be intimately involved in how it is protected.

For agencies, it's about managing security risks and understanding what risks they are willing to accept and how to mitigate risk that falls outside of that scope. That's why it's critical for agencies to work closely with vendors and have conversations about security early and often.

"We've spent a lot of time and resources preparing Software-as- a-Service (SaaS) offerings to meet FedRAMP requirements," Campbell said. "We have a very good idea of the risks associated with our services, and we make that clear to agencies and explain how those gaps are remediated."

When it comes to developing products and services that meet FedRAMP requirements, Cisco is looking far beyond its Webex and hosted collaboration solution.

"We have about 10 other SaaS offerings that we're working on to understand exactly what needs to be done to the applications or operating environments to get them FedRAMP-authorized," Campbell said. "We are culturally, organizationally and financially committed to FedRAMP."

"Our goal is to bring all of our commercially available SaaS offerings through FedRAMP and make them available to our customers who either absolutely require it or have a strong preference for FedRAMP data security," he said.

Conclusion

As with any evolving program, there are kinks in the FedRAMP process that are being worked out over time. The more agencies understand the ins and outs of the program, the better positioned they are to take advantage of all that it can offer.

Well-informed agencies can ensure they are getting the right services that meet their needs and security standards. They can also take advantage of the good work agencies before them have done to verify cloud products and services.

The good news is FedRAMP program officials are coordinating with agencies and vendors to address their concerns about program logistics, resource requirements and continuous cloud security long after the initial FedRAMP approval.

"We see our responsibility as building agencies' confidence in the cloud and cloud security," Campbell said. "We enable their confidence by being prepared and doing our own internal assessments before we introduce SaaS offerings to an agency. We're culturally and organizationally committed to building their trust."

Cisco

Cisco has a broad collaboration-in-the-cloud suite of solutions. Our FedRAMP-authorized solutions provide unparalleled reliability and security with operations and applications, regardless of where they reside.

Today, Cisco offers two core solutions, Cisco Webex Web Conferencing service and Cisco Hosted Collaboration Solution for Government (HCS for Government). Cisco Webex is already a FedRAMP-authorized Service and Cisco HCS for Government is IN PROCESS for FedRAMP authorization. When used together, they provide a complete and secure collaboration solution that was built to meet the stringent requirements of U.S. government-level security.

For more information visit:

Cisco FedRAMP-authorized Solutions for Government
or contact your Cisco representative at
COLLAB-USGOV@cisco.com.

GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information:

For more information about this report, please reach out to
info@govloop.com

1152 15th Street NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421
Fax: (202) 407-7501

www.govloop.com
@GovLoop