RACKSPACE BRIEF

A Simpler, Faster Way to Achieve FedRAMP Compliance For Your Cloud Solutions

Bloomberg estimates that U.S. government cloud spending will grow to over $8.5 billion by fiscal year 2023, creating an incredible opportunity for cloud solution providers to grow their businesses in the government space.

The federal government recognized that the shift to cloud-based technology was the key to IT modernization but that it also opened agencies up to greater security risks. Hence, the development of the Federal Risk and Authorization Management Program (FedRAMP), which provides a standardized approach to security authorizations for cloud service offerings.

Cloud solution providers need to meet the government's criteria for security if they want to succeed, but the FedRAMP authorization process is long, complex and expensive.

The FedRAMP Foundation

For many small and mid-sized companies especially, it can seem like an overwhelming effort to understand the requirements and the projected time and cost involved in achieving FedRAMP ATO. To simplify the discussion, let's break the journey it into three components – **technology, people and process.** Solutions providers have a technology, but it is the process (including requirements) and the people who do the work through every phase of the process (as well as ongoing management) where the complexity, time and costs are heavily impacted.

However, there are ways to simplify and accelerate the process by leveraging external resources like Rackspace Technology. Rackspace is a FedRAMP security and compliance specialist with the expertise, resources and technology to assist with tasks like readiness assessments, managed services, managed security and compliance reporting for FedRAMP accreditation. Rackspace greatly reduces the complexity, level of effort, time and costs to achieve FedRAMP ATO.

Here are three key ways Rackspace Technology can help you achieve a simpler, faster, and more cost-effective approach to FedRAMP authorization:

#1 #2 #3

Start with a Baseline Assessment

Automation doesn't require a reduction in staff; it only means that their tasks change. As with the onset of computerization, workers just have to learn new skills. Agencies can make better use of staff members' creativity to solve critical, rather than routine, challenges.

There are other reasons to automate. Environments are bigger and more complex every day. This generates more and more value, but it also creates more noise and gaps in our ability to monitor the system and new attack vectors. AI solutions play a vital role in cybersecurity. They never get tired and are very good at sifting through the noise to focus on areas of potential concern so they can detect, monitor, and stop cyber threats before they happen.

#1 #2 #3

Don't Underestimate the Workload Involved – AKA the "People" Component

Of the three areas of the FedRAMP process – People, Process and Technology – the "people" component for many is often the most challenging. Organizations tend to underestimate the amount of effort by security, engineers, developers and other IT and business team members to required to manage the processes, procedures, policies and documentation required to achieve a FedRAMPcompliance. The government wants to know in detail how your application works, how your solution operates, and how it connects with other systems. The final application, which can include nearly 1,500 pages of documentation, involves a tremendous workload.

The process already takes time, but it can slow down even more when businesses task already busy developer teams with gathering and documenting the required information. The fact is that few organizations have the in-house expertise to manage the FedRAMP process cost-effectively. Every time the government requires you to rewrite or modify documentation, your costs add up.

You can know your application and how it will contribute to an agency's mission, but to get FedRAMP authorization, you also need people who know how to create policies and procedures that will meet government agencies' specific security criteria.

Moreover, companies pursuing FedRAMP ATOs often underestimate the level of coordination required to meet compliance, especially for large, complex solutions. For example, consider the requirements around password complexity. Those requirements must be implemented at the level of the network, the application, and the database. In other words, one control has an impact across multiple levels of the technology stack, which means that team members from across the organization must coordinate so that everything is configured to meet the required criteria. And then they must manage and maintain security and compliance controls continuously to meet changing government requirements and meet yearly FedRAMP audits.

Rackspace Technology has a team of more than 500 U.S.-based people dedicated to government security and compliance and Rackspace Government Cloud, our platform-as-a-service (PaaS) available on AWS or VMware. From continuous monitoring to vulnerability management to patching, to audit logging and more, they help you as an extension of your own team to manage the "people heavy" processes and requirements and cost-effectively accelerate the FedRAMP process.

#1 #2 #3

Accelerate the Process - Inherit Most of Your Security Controls

As you build the business case for your application, consider the security and compliance controls required by FedRAMP and how you'll achieve meeting and maintaining them. Depending on the level of FedRAMP certification, you could be responsible for more than 400 controls, which can add significantly to the overall time and costs invested in the process.

Nonetheless, business too often attempt to build an infrastructure from scratch and take on FedRAMP certification without help or guidance. Instead, they should work with technology providers who can help them not only avoid mistakes but accelerate the process.

One way this happens is through "controls inheritance," which allows you to shift responsibility for the majority of the required controls to your technology partners. Controls inheritance is an efficient and cost-effective way of meeting FedRAMP compliance, because it allows you to focus your compliance efforts on a smaller number of controls. You essentially piggyback on the investments made by your technology partners and use those authorized controls to accelerate your time to market.

Rackspace Technology is a leader in helping cloud solution providers automate FedRAMP compliance with the Rackspace Government Cloud (RGC) available on your choice of public (AWS), private (VMware) or hybrid cloud Infrastructure-as-a-Service. RGC is a fully managed, zero-trust secure, FedRAMP-authorized PaaS with inherited and managed security controls. With Rackspace Government Cloud, you get automation, security and multicloud adoption expertise that can have you FedRAMP ATO-ready in just three to four months, at 70% monthly operational cost savings — faster and at lower cost than implementing on your own.

And, with approximately 80% of FedRAMP ATO security requirements addressed in Rackspace Government Cloud, our customers reclaim time and resources that can be used to focus on innovating the application layer in support of the mission of government. Rackspace Government Cloud embedded security controls accelerate your cloud solution's time to value, while maintaining full compliance with your cloud security strategy.

About Rackspace Government Solutions

The Rackspace Government Solutions portfolio offers unparalleled multicloud, security, and compliance expertise to empower IT companies to confidently design, build, manage, and optimize the cloud to deliver compliant solutions to the government. As a result, they can accelerate innovation and agility – and meet organization priorities and mission requirements faster. Rackspace Government Solutions enables customers to focus on being technology experts.

RACKSPACE AT A GLANCE

- Leader: 2020 Gartner® Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide
- Leader: 2020 Forrester® Wave for Mulitcloud Managed Services Providers
- Leader: 2020 Forrester® Wave for Hosted Private Cloud Services in North America and EMEA
- 10,000+ certifications across 45 technology logos including AWS, VMWare, Microsoft, Google, Dell, Oracle, and RedHat
- 3,900+ cloud experts including highly skilled engineers, solutions architects and project managers
- Serving 27+ U.S. federal agencies
- Powering 15 FedRAMP ATOs and numerous government cloud solutions
- Servicing the largest public multicloud contract at the state agency level
- The largest AWS global managed service provider (MSP)
- Google Cloud Platform's first MSP
- The only company to establish a VMware Cloud in AWS
- Dell Titanium partner
- A top Azure partner

SECURITY & COMPLIANCE EXPERTISE & EXPERIENCE

- FedRAMP JAB authorized
- DoD CC SRG IL4 authorized
- DFARS/CMMC authorized
- FISMA High authorized
- NIST 800-53 Moderate Baseline
- NIST 800-171 DFARS ready
- CJIS, ITAR, and FIPS 140-2 compliant
- HIPAA compliant
- 24x7x365 SOC, staffed by U.S. team
- TAC 2020 compliant
- IRS Publication 1075 compliant
- Always-available, secure business continuity/disaster recovery capabilities measured in seconds
- A CMMC Registered Provider Organization

For more information about achieving FedRAMP compliance for your cloud solutions, please contact us:

RGS@carahsoft.com
(703) 871-8587
carahsoft.com/rackspace-government-solutions