SECURITY AND COMPLIANCE PROVIDERS SPEED TIME TO ATO

John Lee
Vice President of Cloud Solutions, Carahsoft

The Federal Risk and Authorization Management Program (FedRAMP) offers agencies the assurance that approved cloud services and products meet the government's rigorous security standards. Although efforts have been made to streamline the process, achieving a FedRAMP authority to operate (ATO) is still a multi-layered, time-consuming process that can be challenging for companies to navigate.

It begins with finding a sponsor that will shepherd a cloud product or service through the process. Companies can pursue either an ATO through an individual agency or a provisional ATO through the FedRAMP Joint Authorization Board. A provisional ATO gives an agency a springboard to authorize a cloud product or service for use at that agency.

Next, companies must document every dimension of their cloud technology, which must be configured according to detailed specifications. If a company wants to reach Defense Department customers, it must go through an additional evaluation to ensure that its product or service complies with DOD's Impact Level 4 or 5.

Fortunately, some companies that have automated the process to obtain authorizations serve as FedRAMP Security and Compliance Providers for others that are new to the government market. Their best practices include automating nearly every aspect of the authorization process and building government-approved security platforms that serve as the base on which their partners' applications can run.

Here are three companies that are helping cloud providers achieve ATOs quickly, efficiently and cost-effectively so that agencies can have faster access to innovative technology without compromising security.

Automating the authorization process

Andrew Plato
CEO, Anitian

THE MORE WE SEPARATE THE PURSUIT of security and compliance, the more we end up with environments that are neither secure nor compliant. The solution to this is automation. When security and compliance are an integrated, automated component of a cloud environment, they become more reliable, more consistent and less expensive.

Anitian has taken that idea and built a security and compliance platform that automates the deployment, configuration and certification of cloud environments. In about an hour, our platform deploys an entire cloud environment that is pre-engineered to meet compliance frameworks such as FedRAMP, DOD SRG, PCI, CJIS and more. The platform then wraps a whole suite of security controls around a customer's applications to dramatically accelerate the security and compliance process.

For example, Smartsheet, a well-known software-as-a-service company, already had many federal agency customers for its SaaS workflow management offering. However, it needed to obtain FedRAMP authorization while also moving its products and services into the cloud at the same time. Anitian helped Smartsheet shift its applications into Amazon Web Services' GovCloud, implement all the FedRAMP security controls, document its entire environment and become audit-ready in 58 days. The company received its FedRAMP ATO a few months later.

Since then, Smartsheet's federal business has grown significantly. This is an excellent case study where security and compliance were transformed from an impediment that slowed down business to an energizing catalyst that promotes growth and prosperity. ■

Andrew Plato is CEO of Anitian (anitian.com/fedramp-compliance-automation).

Partnering with a cloud compliance expert

Scott Chapman
President, CEO and Co-Founder, Project Hosts

PROJECT HOSTS MAKES IT MUCH EASIER for federal agencies to grant ATOs to cloud applications. For an agency-dedicated application deployment, initial onboarding to ATO typically takes two to three months. For a multitenant application to get a software-as-a-service (SaaS) FedRAMP authorization, the time is typically six months.

These shortened timelines are only possible due to the fact that Project Hosts has built a FedRAMP-authorized platform as a service (PaaS) on top of Microsoft Azure that covers 80% of all FedRAMP controls and can accommodate almost any application without redevelopment. To grant an ATO, agencies can leverage the already authorized PaaS package and focus their attention on how Project Hosts has implemented the application-specific controls in the remaining 20%.

Project Hosts' PaaS also has an Impact Level 5 authorization that reduces Defense Department ATO timelines to four months.

For an independent software vendor seeking a FedRAMP authorization for its multitenant application, we know exactly what to ask to create compliant control responses. Based on those insights, we have built documentation templates and technical questionnaires, as well as training that prepares application developers for the audit process.

Project Hosts manages about 12 cybersecurity audits per year, so we know what agencies and FedRAMP are looking for. Earlier this year, the FedRAMP Program Management Office told us that its validation of the FedRAMP SaaS authorization package we brought through was the fastest they had ever performed. ■

Scott Chapman is president, CEO and co-founder of Project Hosts (projecthosts.com/government).

Delivering innovation and consistent security

Brad Schulteis
Senior Director of Government Solutions, Rackspace Technology

THE BEST WAY TO CUT DOWN on the time, cost and complexity of the ATO process is by capitalizing on capabilities that already exist. Instead of having to interpret a security control, implement it in a certain way, work with consultants and auditors, and then get the government's approval, companies can use Rackspace Technology's security controls and move on to other requirements.

We offer Rackspace Inheritable Security Controls as a service so that our partners inherit up to 80% of the requirements to get a FedRAMP ATO at the moderate level. In addition, we have 12 authorizations for solutions that run on top of our secure platform.

Many innovative cloud solutions were not built with the government's security guidelines in mind. To achieve FedRAMP approval, those companies have to refactor what they've already done and add security controls after the fact, which is an onerous process. Although companies could pursue FedRAMP authorization on its own, they can reach agency markets much faster by partnering with Rackspace Technology.

We believe in the FedRAMP process, and we believe the software-as-a-service model is ideal for government IT decision-makers. Our goal is to help more companies make it through the FedRAMP authorization process so that we can deliver innovation to the public sector. By providing the government with more choices and consistent security, the government wins, industry wins, and taxpayers win as well. ■

Brad Schulteis is senior director of government solutions at Rackspace Technology (rackspace.com/fedramp).