FedRAMP Ensures Secure Cloud Capabilities

FedRAMP has been working to develop the Open Security Controls Assessment Language (OSCAL). It's implementation will enable agencies and cloud service providers to automate their packages.

The Federal Risk and Authorization Management Program (FedRAMP) continues to play that critical role — the nexus between agencies who are moving to the cloud and the cloud service providers who are innovating with this great technology. Since FedRAMP's establishment 10 years ago the program has seen steady growth. Through this partnership with agencies and cloud service providers, we've been able to authorize over 250 cloud services available in the FedRAMP marketplace. Those 250 cloud services have been reused over 3,800 times to date.

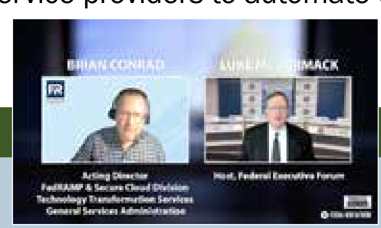
Brian Conrad
Acting FedRAMP Director and Program Manager for Cybersecurity
GSA

As demand grows my challenge is to scale up the program as agencies rush to incorporate cloud services. The critical role that FedRAMP plays is to ensure that the agencies have secure cloud services to use. We are doing really exciting things including plans for automation of not only how we handle packages, but our internal business processes. The bottom line is we're going to continue to grow the marketplace to make sure the agencies have secure cloud services to use, all the while keeping our communications and stakeholder outreach.

Automation Efforts

FedRAMP has been working to develop the Open Security Controls Assessment Language (OSCAL) and its implementation will enable agencies and cloud service providers to automate their packages. Packages upwards of 800 pages get very unwieldy; so being able to automate the package doing validations prior to it coming to an assessor in the government is huge not just for the agencies, but for the cloud service providers as well.

FedRAMP also published a threat scoring methodology for controls against the Mitre attack framework. Why this is important is because the scoring methodology compares the control scores against the Mitre attack framework on how well how well they detect protect and respond to incidents.



Conrad on the Federal Executive Forum

- **Progress Made**
- **Profiles of Success**
- **Priorities**
- **Lessons Learned**
- **Vision for the Future**

What we've been able to do with the NIST 853 Rev 5 controls is to publish their baselines and typically the Joint Authorization Boards (JAB) adds controls on top of the published baselines to make the baselines more applicable to cloud. What we've done in our draft for Rev 5 baselines is comparing that threat based methodology against those additional controls that are typically added to see how well they actually do their job in supporting cyber security. In our draft baselines we've actually been able to reduce the number of controls in the FedRAMP high and moderate baselines which translates into a significant value for not just the cloud service providers, but for the agencies as well.

> In two to three years I envision the FedRAMP program to have our automation capability operational so when packages are submitted, we don't have assessors running through 800-page documents anymore.

All of our modernization efforts are focused on internal business processes that are 10 years old, giving us the opportunity to use automation to reevaluate our business processes. This makes sure that we're being more transparent so cloud service providers can understand where their package is in the process. Also this helps agencies to understand how things are going.

Fully Capable Future

In two to three years I envision the FedRAMP program to have our automation capability operational so when packages are submitted, we don't have assessors running through 800-page documents anymore. We have web APIs established so cloud service providers are pushing their kanban software scans into our platform and that information is being presented through a dashboard. Kanban is a popular framework used to implement agile and DevOps software development. It requires real-time communication of capacity and full transparency of work. Work items are represented visually on a kanban board, allowing team members to see the state of every piece of work at any time.

The dashboard will be updated more frequently than the present monthly updates in regards to the JAB. We want to see that frequency increase so it gives the agencies better evidence to make decisions.

We are being purposefully slow and deliberate on on how we automate, because we're setting the foundation for the program for the next five to ten years. But I would expect in the next two to three that our automation capability will be operational and we'll see so our our authorization timelines for the JAB be around 4.5 months.

There's going to be a point where we can't go any lower because we have to put the rigor behind the assessment. It's critical that we cannot increase the velocity to the point where we are sacrificing the veracity of the assessment. ■