The Federal Risk and Authorization Management Program (FedRAMP) began in 2011 to ensure the government is adopting secure cloud services, and has since helped move government IT workloads to the cloud from antiquated systems. Yet as the FedRAMP marketplace catalog grows and agencies continue to adopt public/private cloud-based services, multi-cloud and hybrid IT environments become harder to manage with existing tools.

Government and industry leaders spoke at a recent FedInsider roundtable to discuss FedRAMP’s impact on enterprise service management, digital transformation and IT security. The following are some of the most important aspects of their discussion.

**Evolving Guidance and Directives**

The Office of Management and Budget issued new FedRAMP guidance, Binding Operational Directive 22-01, which requires agencies to remediate any vulnerabilities outlined in an established Cybersecurity and Infrastructure Security Agency-managed catalog of known exploited vulnerabilities. This poses new compliance challenges for agencies. West Coile, assistant director of the Center of Enhanced Cybersecurity at the Government Accountability Office, said security comes down to knowing what to secure, from what, for how long and at what cost. And for large federal agencies, knowing what they’re trying to secure is already difficult.

“Agencies have to have a good inventory of what they’ve got on premise or in the cloud and visibility is really the key,” Coile said, “regardless [of] whether you outsource some part of your technology stack.”

Automation for collecting inventory from hardware, software and configuration is vital, and networks and inventories are dynamic. That’s where the Department of Homeland Security’s Continuous Diagnostics and Mitigation (CDM) program comes in. CDM is big on asset management, Coile said, “you have to know what you’ve got in order to secure it.”

GAO and inspector general reports show CDM adoption is still a work in progress and remains a challenge for agencies. Visibility of where data and applications reside is the first step. Then, once agencies know what they have, automation is necessary for security practices like patching, validation of patch status and configuration enforcement. This allows IT to become more agile and deliver services more frequently, which in turn leads to resilience.

**FedRAMP and Visibility**

Visibility is a recurring theme in 22-01, and an important component to fulfilling FedRAMP’s new guidance. Brian Conrad, acting FedRAMP director and program manager for cybersecurity at the General Services Administration, said cloud is a shared responsibility model, requiring visibility from all parties. That includes third party assessment organizations, agencies and agency partners.

“FedRAMP, we sit in a unique place between the agencies who are moving to cloud and wanting to use this great technology that the cloud service providers are developing, and on the other hand, we have the cloud developers that are pushing the envelope with technology,” Conrad said.

Visibility requires all parties to understand their role, each other’s roles and the fact that cybersecurity is a team sport. “There’s a FedRAMP standard that clouds need, the cloud providers are doing everything to protect federal information,” Conrad added.
Third party assessors are validating, the FedRAMP Program Management Office is setting policy, and both are working in concert with government agencies, entities, OMB and the Joint Authorization Board. Conrad’s office, for instance, shares and communicates the role FedRAMP plays in federal cloud adoption as its commitment to visibility so commercial cloud providers know what to expect.

FedRAMP also ensures that the administrator has controls in place. Monitoring those controls is also related to visibility. Cmdr. James Jones IV, director of the cybersecurity division for the National Oceanic and Atmospheric Administration, said understanding the mission, organization, module and controls all tie in with one another.

The SolarWinds hack, for instance, brought to light processes and procedures NOAA needed to update to ensure it had proper visibility. So, along with the tools NOAA adopted to accomplish that, visibility of controls is critical. “It’s so important that the practitioners . . . whoever the responsible party is over the cloud service providers and the organization’s security controls, that they stay in constant communication,” Jones said, to ensure controls are lined up with what is seen from the security operations center.

While having a hybrid cloud environment makes visibility into these environments more challenging, good asset management practices and a reevaluation of existing tools will help. It’s important IT leaders plan for interoperable and portable applications as part of their hybrid cloud environment, so it can adapt with innovation and continue to meet security requirements as they evolve.

**Updating Tools with FedRAMP Marketplace**

Commercial and federal organizations frequently use accessible tools to adhere to new mandates. But just because one tool is working in one circumstance, doesn’t mean it works for another. That’s where FedRAMP Marketplace comes in.

Conrad said the marketplace includes over 250 authorized cloud services that federal IT leaders can go to find a cloud service that serves a specific need. “That’s a time efficient method in and of itself to help federal leaders come to conclusions on which cloud services may be suitable for their organization,” Conrad said.

And considering the increased adoption of hybrid cloud environments, Kevin Hansen, public sector chief technology officer at Micro Focus Government Solutions, said training staff on multiple tools to achieve the same outcome can be costly and inefficient.

“It may be a sign that your tools are not sufficient to support the enterprise,” Hansen said. “When tools are agnostic to the run time platform, the infrastructure, and your cloud providers, you can achieve flexibility.” That, in turn, enables enterprise services with more automation, analytics and a clever view of IT assets. And it delivers more value to IT and the mission.

**The Key to Cybersecurity in Government Is Collaboration**

“Collaboration . . . the philosophy and the concept is so important in this context as well as broader scale cybersecurity in order for us to be as resilient as we can and become a strong nation together,” said Jones. And Hansen agreed, noting that collaboration and communication across different IT domains is usually key to being successful.

GSA has its Center of Excellence programs for this reason — to share best practices and challenges, especially around new technologies, new methodologies or strategies, IT modernization and cybersecurity.

And in terms of cybersecurity, collaboration and communication can help prepare agencies for the possibility of CISA adding guidelines in the future by interpreting guidance, organizational risks, risk posture, shared resources and so on. Strong communication from the top-down leads to proper direction and coordination, agency-wide understandings to implement change, and the granting of proper authorities and permissions to make them happen.