Charting a Course

The clear path that accelerates the move to the cloud

Cloud is transforming federal government, making IT processes more efficient, cost-effective and more responsive to citizens' needs as well as intergovernmental activities. Yet, getting there can be a challenge.

Technical hurdles and procurement processes can stymie cloud adoption. While new initiatives like Cloud Smart help to steer agencies through the complexities of security and privacy in the cloud, many federal IT leaders continue to struggle with the migration of legacy processes into the new environment.

Consider a few of the demonstrated benefits of cloud in federal government, challenges to cloud adoption and key strategic points for helping federal IT leaders steer organizations toward a cloud-driven architecture.

Federal agencies are reaping substantial gains from cloud computing. The Government Accountability Office reports that investments in cloud services by13 agencies have saved a total of $291 million since 2014. Officials representing 15 of 16 agencies told GAO that cloud provided "significant benefits," including improved citizen service and cost-effective IT management.

As federal agencies seek to clean up piecemeal IT environments, cloud provides an opportunity to streamline those fragmented operations. Agencies are using cloud to identify and consolidate previously scattered application development efforts, thereby eliminating redundant costs and streamlining validation tools and other aspects of systems management through consolidation.

Consolidation in turn nudges agencies towards an agile development environment. Cloud allows IT leaders to rapidly change the development, test and production environments, enabling them to pare development cycles down from months to days. On-demand capacity of this sort can drive organizational change.

Despite the benefits of cloud adoption, some federal agencies have been slow to commit resources in this direction. GAO reports that just 11 percent of agencies' planned fiscal year 2019 IT investments are targeted to cloud computing services.

That's a two percentage point rise over FY 2017 and 2018 levels, yet the federal government's cloud migration efforts continue to trail the private sector's push to the cloud. IDG, for

instance, reports that private sector companies today allocate 30 percent of their IT budgets to the cloud.

Sluggish cloud adoption on the government side isn't a surprise considering the many hurdles that may impede federal tech leaders seeking to jettison legacy platforms in favor of the cloud.

Cloud hurdles

Many leaders in federal IT harbor concerns about security in a cloud-enabled world. MeriTalk reports that among government tech leaders, 65 percent rate security as a top concern hindering cloud adoption. Sixty-one percent cite migration complexity as another major sticking point, and 60 percent say a lack of visibility hinders their efforts.

The issue of visibility is not trivial. Many feds find it hard to push the "go" button on a cloud project simply because they don't know what they have in their inventories: It's unclear what systems and processes would benefit from a cloud implementation; they don't know which pieces are cloud-ready; and they frequently don't have access to the needed documentation that would help to answer these questions.

Developers within federal agencies may have structural challenges, such as the lack of secure remote access. Other hurdles include federal procurement processes that aren't friendly to purchasing IT as a service. Government has taken steps to remedy this issue, such as Governmentwide Acquisition Contracts (GWACs), but procurement processes remain a sticking point.

There is nonetheless a clear path forward for agencies looking to take advantage of the speed, scalability and improved efficiencies available within the cloud environment.

The way forward

Government has put in place a number of key mechanisms to smooth the path. The Federal Risk and Authorization Management Program (FedRAMP) spells out a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The Department of Defense Cloud (DoD) Computing Security Requirements Guide (SRG) does much the same for military users.

These tools are under-utilized. A survey by the Ponemon Institute, for instance, found that only 43 percent of cloud providers within agencies are FedRAMP authorized, while 69 percent of respondents said that over half their cloud applications are not FedRAMP authorized. Greater FedRAMP compliance and adoption of the DoD SRG are a key first step in accelerating federal cloud projects.

IT leaders also can look to the recently released federal Cloud Smart vision for guidance. Cloud Smart's guiding principles encourage government technologists to look at reskilling and retraining staff, enhancing security postures, and using best practices as potential pathways toward cloud adoption.

Beyond this, federal IT leaders can leverage a high-level approach to organizational change management as they seek to deploy cloud-based projects.

For example, federal agencies need to formulate a clear view of their IT inventory and resources in order to move methodically toward the cloud. Applications rationalization is key, as is asking foundational questions: What applications or systems merit investment in people and resources? What processes will benefit most from cloud's speed and scalability? What systems reach across the enterprise and bring greatest benefit to the most users?

Taking stock

A deeper understanding of the as-a-service landscape also can be helpful, as there isn't a single version of "cloud" to suit all purposes. Some processes require an infrastructure platform or a software-as-a-service approach, while others lend themselves to a database-as-a-service solution. In taking stock of which systems are ripe for the cloud, it's useful to consider the type of cloud solutions available.

When it's time to move forward, automation can be a key enabler. Federal agencies can end up spinning their wheels if they rely on manual means to execute a cloud migration. Artificial intelligence and machine learning tools, on the other hand, can bring predictability to the process, delivering an automated means to maximize the cloud investment. Automated synchronization of databases and AI-assisted extrapolation of information can help to minimize the time and effort needed, while ensuring transparency and consistency across the enterprise.

Finally, emerging best practices suggest that federal agencies can best approach the cloud in small steps. Many federal leaders, for example, have realized that enterprise resource planning is a natural fit for the cloud – a massive undertaking with potentially hundreds of interconnected moving parts.

Initially, it often makes sense to pursue more attainable goals. A single development project, for example, can be migrated discreetly and safely to the cloud. Solid funding, clear parameters and well-defined goals make for an easier win. Lessons learned from the first project will inform the next, creating a ladder of success for further cloud adoption.

While the initial projects should be small, the authority should come from the very top. Federal agencies that have made the leap to cloud typically have seen the driving force come from the CIO or CTO, high-level individuals with full budget authority and the organizational clout to see a project through to completion.

The road to cloud is strewn with hazards: procurement hurdles, organizational challenges, technical sticking points. But for federal agencies looking to take advantage of the cloud's inherent benefits, there is a way. High-level leadership, organizational transparency and a commitment to automation can move federal systems and processes into a modernized, shared, highly scalable environment.