MAPPING YOUR PATH TO THE CLOUD

INDUSTRY PERSPECTIVE

Hitachi Data Systems Federal

EXECUTIVE SUMMARY

There's no denying that cloud computing is transforming the way government agencies consume information, deliver services and carry out their unique missions.

Over the past few years, agencies have gradually shifted from owning the hardware and software that support these functions to buying access to IT infrastructure and applications as a service. Early adopters of cloud have reported cost savings and IT efficiencies because they have far fewer assets to manage and greater flexibility to adopt innovative services that can be accessed more broadly from various devices.

Government-wide efforts such as the Federal Risk and Authorization Management Program, or FedRAMP, have played a key role in speeding adoption of secure cloud services. The program brought much-needed standards to cloud security by providing a common baseline by which agencies can determine if a cloud product or service is secure for government use.

For vendors, FedRAMP provides common, government-wide standards they can build to and use to show their solutions are fit for government use. Although FedRAMP launched as a federal program in 2012, a growing number of state governments are using the standards to vet security of cloud offerings.

But as with any new way of doing business, there are a few challenges. When it comes to adopting cloud services, there are three obstacles in particular that agencies can attest to: budgeting, procurement and organizational challenges.

First off, organizations have to budget for a cloud service much like a utility service, and agency buyers expect to pay only for the services they use. Second, agencies also have to navigate the challenges of buying services as opposed to assets. Then there's the organizational impact of moving to cloud, especially when it comes to roles and responsibilities for the agency and contractors.

These are just some of the common issues agencies face. There's also the challenge of deciding if your agency is ready for the cloud, which deployment model to use and how to develop a thorough migration strategy.

To help agencies answer these three key questions, GovLoop sat down with Rob Davies, Executive Vice President of Operations at ViON, an IT Enterprise Solutions Provider. In this report, we'll explore these questions and provide best practices for overcoming common challenges. But first, let's start by addressing a question every cloud user must weigh: How ready are you to embrace cloud?

HOW READY ARE YOU TO EMBRACE CLOUD?

Are you ready for cloud? For agencies that want to get out of the business of owning IT resources, the short answer to that question is likely a resounding yes.

"I think everybody in the government can benefit from a cloud model because every agency could use greater predictability in their budgets, an ability to meet a surge in capacity, the ability to have a consistent and reliable disaster-recovery strategy and modernization in their organizations," Davies said.

It's not so much a question of whether you should move certain applications to the cloud, but when and more importantly, how.

But Davies also noted that cloud readiness is about much more than a desire or need to adopt cloud services. The real question is: How do agencies know which applications are ready and what workloads are the right ones to move to the cloud?

Some of the greatest barriers to cloud readiness don't involve the technology. Often, the issues are misunderstanding, fear and anxiety. To help ease any fears and inform potential cloud buyers, Davies offered these five tips to prepare for the cloud:

Start small.

Use a development environment to better understand how an application is supported before moving it to a cloud environment. If you haven't done an analysis of that workload or application, you don't know what interdependencies exist between applications and whether moving them out of your enterprise will affect how they perform.

Focus on non-critical applications first.

Ideally, you don't want to do a technology refresh for a large system and then opt to move it to the cloud. Consider starting with a system that isn't critical to performing your agency's mission and then evaluate more critical systems. Again, a development environment can help you better understand how the app performs in the cloud.

Consider virtualization.

Legacy applications in a mainframe environment aren't the best candidates to port directly to the cloud because they are older systems that are not modernized to function well. On the other hand, if you have a virtualized environment running VMware or another hypervisor, you could be on the road to cloud readiness for that system. However, you still need to do an assessment of your operational environment and determine if it's a likely candidate for cloud.

Ensure cloud vendors talk specifics.

When you're talking to vendors about cloud readiness, require that they talk specifics. For example, have them walk you through a checklist of the types of requirements that you want met when workloads move to the cloud.

Do a thorough assessment of your operational environment.

This should be done across all applications to determine the characteristics of all apps, their workload performance, what types of software and what versions those applications are using, as well as the platform they're running on.

"Our definition of cloud readiness is about being ready for use, and we help agencies through this process," Davies said. "That means you've migrated, you're up, you're ready to go and you can turn that over to your user base, wherever they are."

WHAT'S THE RIGHT CLOUD FOR YOU?

There's no shortage of cloud services and options for how to manage and host them, whether in-house or in a third-party facility.

But even before that's decided, agencies have to consider which applications can and will move to the cloud.

"It really is about the importance of the system, but that can be hard to determine," Davies said.

Here's why: If you were to solicit employees at any organization and ask about the importance of various applications, everyone will say their application is important. But in reality, there are tiers of importance.
For example, let's say you're the head of a fee-for-service agency. You have a major mission application that does all your transaction processing of different charges. And you use this system to collect revenues.

That's probably not the system you're going to put in the cloud first. That may be the last thing you put in the cloud, or you may not put it in the cloud at all. But then there are other systems and applications, such as public websites, that customers use to interface with your agency and pay their fees.

There are elements of that application you may put in the cloud, but the backend system and user data may be stored on-premise. The key questions cloud buyers should answer when deciding what type of cloud best meets their needs are:

What do you need to manage?

Similar to the earlier example, there are some applications in government that will never move to a cloud environment because they are inherently governmental functions that cannot be performed by a contractor, or agencies aren't willing to accept the risk associated with moving a particular data set or application to the cloud. Security requirements often dictate the type of cloud that agencies use. For risk-averse agencies, a viable option may be a private cloud, where the cloud infrastructure is provisioned for exclusive use by a single organization. The cloud may also be owned, managed and operated by that organization. Either way, security must be addressed.

Who is the end user?

Are the people using the service employees at your agency or are they employees at another agency who are sharing the service? Maybe citizens are the end users. Understanding who will use the service also affects cloud selection. For example, a public website or portal may be a great candidate for a public cloud, but maybe the actual system that stores any personally identifiable information citizens share is hosted in a private cloud or not in the cloud at all. For groups of users with a shared mission and common interests, such as the intelligence community and research institutions, community cloud is proving to be a viable option.

What can someone else manage?

If a third-party vendor or another government agency can manage the service, then that creates more options. Rather than only considering a private cloud, there may be an opportunity to explore the other models as well, including a public cloud, hybrid cloud or a community cloud. But the type of end user and the sensitivity of the data being stored in the cloud will influence this decision.

What type of data would be in the cloud?

The sensitivity level of the data will play a major role in selecting a cloud deployment model. For example, the Defense Department uses "impact levels" to classify the sensitivity of its data and determine which cloud environments are most appropriate to meet its security standards. The impact levels are defined by the sensitivity or confidentiality level of information (whether it's public, private, classified, etc.) that will be stored and processed in the cloud and the potential impact of an event that results in the loss of confidentiality, integrity or availability of that information.

This is where programs like FedRAMP play a major role in determining how certain data should be secured in the cloud. FedRAMP standards also help agencies determine if a particular cloud deployment model is appropriate to host different types of data.

Agencies must keep in mind that these questions should not be considered independent of one another. They all play a collective role in assessing what type of cloud can best meet their needs.

"When deciding what applications to move to the cloud and what type of cloud model to use, consider what the application does," Davies said.

That helps you understand the applications that are most important to your business and the applications that are furthest away from it. Applications that are not central to your mission and can be easily migrated to the cloud are good candidates to test in the cloud.

To help ease the load of adopting and implementing cloud services, some agencies have turned to cloud brokers. These organizations serve as intermediaries between cloud buyers and cloud sellers and provide added value in various areas, such as cloud procurement and negotiation as well as implementation. Cloud brokers can be private companies or government agencies.

"There are a lot of cloud brokers out there now that can come in, take a quick look at your workload and help you decide where to go and what to do," Davies said. "I don't think there are a lack of resources for agencies to go to the cloud. Sometimes it's a matter of selecting a service and starting the process."

Critical vs. Non-Critical Applications

Cloud migration is generally standard for most applications — both critical and non-critical. Critical apps are those that are central to your mission and require high availability. In some cases, mission-critical apps may be better candidates for the cloud, particularly if they are newer and modernized. But they shouldn't be the first candidate because these systems need to be up and running all the time.

It's good to start small, experiment and use those lessons learned to migrate critical apps to the cloud in the future, if that aligns with your agency's IT strategy. If and when you decide to move critical applications to the cloud, consider that newer apps still require development, quality checks and user testing before they are hosted in a cloud environment.

WHAT'S YOUR MIGRATION STRATEGY?

Migrating to the cloud isn't a one-time event — it's a journey. Preparation and thorough planning are key to mapping out a successful path to the cloud.

Before applications are actually migrated to the cloud, agencies must first define their solution, develop requirements, procure the solution and ensure it is secure.

"When you get to the point where you're actually migrating to the cloud, the steps really aren't much different than bringing any other application into production," Davies said.

Regardless of the type of development methodology agencies use — agile being one example — they need to have a checklist of all the functions that must be completed before the final launch. This may include standing up a quality assurance environment to do load testing on the cloud and ensure the servers and other resources selected for the cloud are adequate.

The migration process may also include user acceptance testing to check and address any features that have changed and ensure response times for websites meet service-level agreements defined in the cloud contract. During this phase, there may be kinks that need fixing.

"One of the last things before you actually turn on the solution in production is the go-live exercise," Davies said. "In this stage, you simulate a live user experience, using people who have been part of the process, and they can test it out and take note of what needs to be changed or fixed. Once those changes are made, you can go live."

Whether you're moving to a public or private cloud, the vendor should have resources to help you get to that end state. There are cloud contracts that make clear vendors cannot start the billing process until customers have reached a certain stage in the cloud migration process. So there's an incentive for vendors to get applications operating in the cloud as quickly as possible.

"The application has to operate and perform accordingly, or else vendors don't get paid," Davies said. "We structure our contracts to ensure we as the vendor can meet the service-level agreements. That's another important issue to address when considering a cloud solution."

Davies advised that government acquisition officials be involved in meetings and discussions with vendors to address requirements and costs. There should also be a clear and documented exit strategy for ending the service and any associated costs that may include.

"You have so many different variations of cloud, so there has to be a barometer against which the government can say, 'I'm getting a reasonable price because of these factors,' and maybe that's comparing it against what traditional spending would be and showing savings," he said.

Another option is the General Services Administration's hub for acquisition professionals to share and explore historical prices paid data, lessons learned and other helpful information on a range of products and services, including cloud.

LOOKING AHEAD

Cloud computing has reached a point of high reliability and economics, and it should be considered along with any other technology.

In fact, federal agencies and a growing number of states are required to consider secure cloud options first when buying new technologies. The promise of greater efficiencies and cost savings make cloud an appealing option, even for risk-averse agencies like DoD.

"The budgets don't exist anymore to hire a contractor and a program management group to design a system, evaluate it, procure all the hardware, integrate it and develop an application," Davies said. "That takes too long."

Government employees and the citizens they serve expect agencies to operate like private companies and deliver better services faster. Cloud is that enabler.

"Cloud allows you to turn resources on or off, acquire new resources faster, quickly get rid of something you don't need, and you don't have to pay for services you don't use," Davies said. "It gives you flexibility and speed."

In terms of costs, agencies should always evaluate the cost of a system throughout its lifecycle and compare that with the cost of hosting that system in the cloud. Cost and capabilities should be a part of the frank conversations agencies have with vendors.

"Customers need to be able to question the vendor, and the ones that have that specificity, that means they're experienced and they have the workflows and processes in place," Davies said.

Davies noted that there are still privacy and security concerns that government agencies are working through, but progress is being made. "I think we'll move past most of those arguments, and cloud is going to become a necessity because the technology is there."

The reason: Cloud enables IT Innovation. It enables government agencies to focus on achieving results instead of worrying about the technology.

ABOUT VION

Designing and implementing innovative solutions that meet dramatically changing IT requirements is ViON's mission. Founded in 1980, we've grown from a small product reseller into a leading systems integrator delivering customized solutions and best of breed offerings from the world's premier OEMs to large public and private organizations.

Known for our engineering expertise and exacting standards, ViON ensures that only those with the highest level of training, experience and industry certifications design, install, maintain and support our breadth of solutions.

We focus on data management, so you can focus on your organization's success. We're on the leading edge of Big Data and Cyber Analytics, Cloud, Video Surveillance and Storage. ViON's cloud-based "as a Service" Program Management Office delivers direct access to the technology you need for today and tomorrow.

From the data center to the cloud, let ViON's passion for innovative solutions secure the competitive advantage required for your enterprise. Learn more at www.ViON.com.

ViON
Building your enterprise solutions

Hitachi Data Systems Federal

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

govloop

1152 15th Street NW, Suite 800 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop