AKIMA

WHITEPAPER

Best Practices in Cloud Migration: The Why, the When, the How

Moving data center assets to the cloud is a sound move for agencies of all sizes that can nonetheless be complicated, slow, and confusing. Following a few best practices, however, can make for smoother migration, resulting in efficiencies, cost savings, and agility that ultimately make it easier for agencies to advance their missions.

The Why

Best practices represent wisdom accrued by agencies that have gone there and lived to talk about it. In the realm of cloud computing, these experiences are particularly valuable at a time when more and more federal workloads are moving to the cloud. Cloud migrations are not a new concept; however, they started at a time when agencies were only beginning to get comfortable with the concept of "as-a-Service."

Today, "as a Service" is everywhere, and agencies are moving data center assets to the cloud at an increasing rate, encouraged by mandates like the Data Center Optimization Initiative (DCOI),[1] and updated guidance from the White House's Cloud Smart Strategy and 2017 Report to the President on Federal IT Modernization.[2] These directives position agencies to move forward with IT modernization by enabling them to add or subtract resources as needed, increasing visibility into assets, and ensuring that agencies always have access to the most effective and current technology resources.

> *In order to aggressively modernize IT systems, the Federal Government will need to maximize use of shared services and commercial capabilities. In furtherance of this objective, existing policies and programs will be rapidly and iteratively updated to eliminate barriers to cloud adoption, and agencies will rapidly migrate applicable capabilities to commercial cloud services.*
>
> – 2017 Report to the President on Federal IT Modernization

Observing best practices when moving to the cloud can be the difference between a smooth transition and a rocky road.

[1] *policy.cio.gov/dcoi*
[2] *itmodernization.cio.gov*

The When

When it comes to data center migrations, timing is everything. However, the "when" might not always be clear. For some agencies, the impetus for cloud occurs when a data center is ready for a technology refresh, or when storage resources are quickly becoming obsolete or otherwise nearing end of life. For others, slower applications serve to provide urgency for moving to the cloud. The bottom line is when a lack of sufficient resources makes it difficult for employees to do their jobs and agencies' to advance their missions, it might be time for a change.

However, before moving forward, agencies should take stock of their current data center infrastructure to determine the best mix of resources for their new cloud-based environment.

"When we work with agencies who are thinking of moving data center assets to the cloud, the first steps is always a cloud-ready assessment. We examine their existing infrastructure, perform an overall health check, and do a gap analysis of the as-is state and the future state," explains John Fair, director of business development for Akima, an Alaska Native Corporation that provides comprehensive IT services to the federal government. "That way we have a roadmap and we know what we need to do before migrating to ensure it goes smoothly."

It is rare for any agency to pass such a thorough assessment with flying colors, Fair says. Instead, the assessment usually uncovers issues that need to be addressed before moving forward. Failing to fix existing problems at the outset can slow the transition to cloud and make the process more difficult than necessary.

"We find a lot of things when we do these assessments," Fair says. "For example, one of our customers had a single switch that was configured wrong, and it was keeping traffic to about 50 percent of what it should have been. That makes an impact when planning for future capacity. We've also found servers that were not up to the latest service pack so they were having memory leaks or SQL databases with sensitive information and no passwords."

Slow network connections and network latency are also very common and should be resolved before moving to the cloud. Most agencies – especially in the Department of Defense – connect to the internet by passing through several network connections, an arduous journey that adds layers of complexity and slows connections. **Akima addresses this issue by creating connections closer to the source.**

> *"When we work with agencies who are thinking of moving data center assets to the cloud, the first step is always a cloud-ready assessment.*
>
> – John Fair, Director of Business Development, Akima

The How

The next step is deciding what type of cloud environment will best suit your agency's requirements and preferences. Typically, there are two choices: a full **cloud-based data center** with everything in the cloud; or a **hybrid data center** in which infrastructure remains on the premises, with the remainder shifted to the cloud.

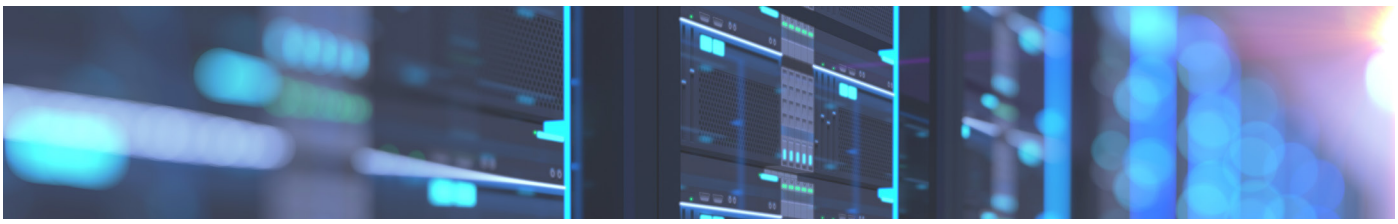
Depending on the agency's comfort level and regulatory requirements, Akima may recommend one over the other. Fair says a cloud-only data center is often best, yet there are times when a hybrid solution is the better choice, he says. It is great for agencies just getting comfortable with the cloud and those that must keep specific data sets on premises for security reasons. Often, he says, agencies start with a hybrid data center and later migrate to a full cloud-based solution.

Before throwing the switch and commencing migration, it is critical to make sure that all backups and recovery systems are working correctly. It is also important to educate staff on the implications of a migration. Knowing what to expect will help employees deal with the changes.

It can also be prudent to build into the process time for a test phase. Doing so allows agency IT personnel to test-drive the system before the full rollout, providing employees time to acclimate and the vendor an opportunity to fine-tune the system.

Always start small.

"We find that starting with non-critical data is a good plan," Fair explains. "Then we move 'up the chain' to things like flat files and home directories. By using this approach, we can start to build trust in the entire process, which is important to overall success of a cloud migration."



Choosing a Vendor

Finding the right partner is critical. Vendors should take the time to understand both your existing data center environment and your desired cloud-based environment, and then work collaboratively to architect the best path to the cloud. Before starting the project, they should also remediate any latency, necessary upgrades or outstanding performance issues. This will help avoid problems during the migration process.

When possible, it is also helpful to limit the number of organizations involved in the migration. Too many vendors can hinder communication and slow progress. Consider partnering with a company that can deliver both the IT products and services you need. Doing so will streamline communications.

To ensure the highest level of security possible, it is also important to insist that your service providers are FedRAMP-certified to at least Level 3. With this level of certification, agencies can be confident that data, applications, and other assets are protected with current IT security best practices, such as encryption, public key infrastructure, and multifactor authentication.

Finally, make sure that the vendor's cloud-centered data center strategy positions your agency to embrace inevitable technological advances, new data types, and changing mission priorities.

The migration process may be finite, yet it is important to understand that a cloud-based data center is, in essence, an evolving thing. To continue its efficient operation, make sure your vendor monitors important metrics, such as throughput and latency, using baseline measurements and metrics against agreed upon service level agreements (SLAs).

Once the migration is complete, set up a system to replicate all data into another cloud – yet another best practice that bolsters security, redundancy, and disaster recovery, Fair says.

Transitioning data center assets to the cloud doesn't have to be painful. By taking the time to understand and follow best practices, agencies can gain the benefits of a modern cloud environment and take another step toward the future of federal computing.

About Akima

Akima and its portfolio of companies are uniquely positioned to help agencies in their journey to the cloud. Our services span the full implementation lifecycle, from pre-sales engagements such as Cloud Readiness Assessments and Proofs of Concept all the way through to post-implementation and support for driving end user adoption and future expansion. We can help agencies evaluate their current environment, plan/prep applications for migration, implement robust cloud security policies following NIST and FedRAMP, and perform testing and Disaster Recovery validation in the new cloud environment.

Whether you are looking for end-to-end services, or support for only a piece of the transition, our cloud experts stand ready to support your efforts.

Learn more at akima.com/cloud.