THREE STRATEGIES TO ACCELERATE YOUR AGENCY’S MIGRATION TO THE CLOUD

Since releasing the Federal Cloud Computing Strategy in 2011, the federal government has focused its technology management strategy on migrating mission-critical operations to the cloud to address an IT environment characterized by poor asset utilization, duplicative systems, and a slow procurement process. The cloud’s potential to enhance federal agencies’ efficiency, agility, and capacity for innovation cannot be overstated. In an era of stagnant IT budgets and a growing capabilities gap between private and public sectors, cloud computing offers the federal government the opportunity to reach an increasingly interconnected and mobile public, as well as to save billions and simplify the IT procurement process.

As is often the case with transitions of this scale, cloud migration has had its share of challenges. In a January 2014 Government Business Council study, 49 percent of federal executives responded that their agency had migrated less than ten percent of its application portfolio, citing concerns over security, data ownership, budgeting, and expertise gaps. Although cloud migration might seem imposing and lend itself to endless strategizing, agencies have demonstrated that they are capable of deploying cloud services in a matter of months, not years. Those most successful have focused on three key areas: selecting high-value and high-readiness applications for migration, assessing their service and deployment needs, and aligning those requirements with available budgetary resources.

Selecting Applications for Cloud Migration

The Federal Cloud Computing Strategy was designed as a reference for how agencies should approach their transitions to the cloud, but it also specifies the criteria that should be used to prioritize applications for accelerated migration: value and readiness. Agencies are more likely to realize value when targeting applications able to make an immediate impact through improving resource utilization, scalability, and customer satisfaction. Similarly, cloud-ready applications have trusted security credentials, are already virtualized or easily virtualized, approaching the end of their lifecycles, and easily separable from other systems.

Going boldly where few agencies had gone before, NASA began experimenting with cloud computing as early as 2008. NASA’s greatest cloud success story came in 2012 in the midst of preparing for the rover Curiosity’s arrival on Mars. To achieve its goal of delivering live video feed of the landing to
the public, NASA required flexibility and rapid scalability of computing resources. CTO Tom Soderstrom selected the agency’s imaging and public engagement applications as high-value, high-readiness candidates for migration. The cloud allowed NASA to seamlessly bring its Mars broadcast to millions of viewers worldwide, and NASA continues to host its user portal via public cloud at costs much lower than on its own infrastructure.

**Evaluating Cloud Service and Deployment Models**

Once an agency selects the applications and capabilities destined for migration, the next major challenge is designing a portfolio of cloud service and deployment models that optimizes its requirements for security, data ownership, and cost savings. Agencies can choose from multiple, distinct cloud tiers based on the expected utilization of those services. Systems administrators might choose infrastructure (IaaS), which includes processing, storage, and networking resources, or platforms (PaaS), which include tools and an operating system supported by the cloud service provider (CSP), in order to develop customized applications for agency personnel. Alternatively, if the primary consumers are end-users, cloud-based software applications (SaaS) hosted by the CSP may supply the most rapidly deployable turnkey solution.

An agency may then choose to deploy a private, public, or community cloud solution. A private cloud is often hosted on-premises and typically offers greater control over sensitive data, while public clouds are managed by the CSP and allow agencies to pay for services solely on the basis of utilization. The following cases illustrate how cloud service and deployment models can vary based on their intended usership and function.

In May 2012, the U.S. Marine Corps (USMC) released its strategy to deploy a private cloud through the Marine Corps Enterprise Information Technology Services (MCEITS) program. The goal of MCEITS is to provide universal access to USMC data and applications, particularly in forward-deployed and potentially hostile environments with severe bandwidth limitations. By choosing a private cloud environment built on top of a commercial IaaS solution, the USMC can achieve optimal security and data ownership, while providing service members with command and control capabilities as well as email, file sharing, and video conferencing. In addition, MCEITS gives USMC administrators rapid access to scale-up or scale-down capacity as needed, ensures savings through resource pooling and data center consolidation, and reduces the manpower needed to maintain its networks.

On the other end of the spectrum, in late 2010 the Department of State chose to deploy a cloud-based electronic library to provide access to documents and country resources stored in databases worldwide. A public SaaS solution was optimal for two reasons. First, the documents were already in the public domain, and based on their low FISMA security rating, required minimal centralized data management. Second, users were primarily domestic and overseas staff members who required minimal custom functionality aside from a self-service check-out tool. By accurately assessing its service needs, DoS was able to deploy the electronic library on-time and at-cost, while meeting all major milestones and performance goals.

“In a 2014 Government Business Council study, 49 percent of federal executives responded that their agency had migrated less than ten percent of its application portfolio, citing concerns over security, data ownership, budgeting, and expertise gaps.”
Aligning Budgetary Resources with Cloud Services

A remaining challenge for federal agencies is deciding how to pay for cloud migration. Of roughly $80 billion in annual federal IT spending, an estimated $20 billion is a potential target for agencies seeking to migrate operations to the cloud. However, only about $3 billion of that total will actually go toward cloud services, according to Office of Management and Budget cloud computing manager Scott Renda, who cited difficulties in certifying CSPs for security compliance and in reforming the way some agencies procure IT. Prior to the cloud era, government acquisitions offices customarily purchased computing, storage, and other IT assets as capital expenditures (CapEx) and must now shift to procuring cloud services as an operations expenditure (OpEx) – similar to a standard utility.

One way agencies have adapted to their new environment is through redesigning contract vehicles to pay for infrastructure, platforms, and software as services. GSA’s IaaS Blanket Purchase Agreement (BPA), for instance, streamlines the purchasing process through eliminating the need for agencies to independently certify potential vendors for cybersecurity compliance, negotiate service level agreements (SLAs), and define data ownership rights. Instead, CSPs pre-compete for contracts for specific IaaS functions including cloud storage, virtualization, and web hosting. If they meet the necessary security qualifications, vendors can be pre-certified by GSA. By centralizing its cloud acquisition process through BPA, DHS for instance, was able to dramatically shrink its infrastructure costs, reduce procurement lead-time, and boost confidence in the security of its cloud data.

Tomorrow’s Forecast? Heavy Cloud Coverage

After three years of deliberate progress following release of the Federal Cloud Computing Strategy, federal agencies are preparing to migrate larger portions of their application portfolios into a wider array of cloud service and deployment models. Despite the fact that 75 percent of government cloud spending remains directed toward private cloud deployment, the public cloud market has matured rapidly since “Cloud First.” As IT security officials gain greater confidence in negotiating SLAs and in certification programs like FedRAMP, public cloud and PaaS will likely begin to comprise a greater share of total spending. In the coming years, federal agencies will face difficult decisions over whether the benefits of migrating older and more complex legacy applications outweigh the potential risks of service disruptions or permanent functionality deficiencies. Similarly, federal, state, and local governments are increasingly looking to cloud brokerage as a more cost-effective means of delivering and managing cloud services.

As agencies continue their efforts to address their cloud challenges, OMB’s Scott Renda reminds federal leaders that they need to plan to expand cloud services as the foundation of their twenty-first century IT architecture: “it’s definitely here to stay, and it’s only going to get bigger.”
Sources

1. The National Institute of Standards and Technology defines “the cloud” as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and servers) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” see: Peter Mell and Timothy Grance, “The NIST Definition of Cloud Computing” U.S. Department of Commerce: September 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Image: techspot.com (labeled for reuse)