Data Center
Optimization Initiative

Key Cost Considerations for Agencies Planning Cloud Migrations

November 27, 2017

Data Center Optimization Initiative, Managing Partner
General Services Administration
Office of Government-wide Policy

Key Cost Considerations for Agencies Planning Cloud Migrations

Purpose and Summary

The Data Center Optimization Initiative (DCOI) Managing Partner PMO conducted non-attributable interviews with officials from federal agencies to understand how costs drive cloud migration outcomes. These individuals offered candid insights into their organizations' cloud experiences, as both service providers and as consumers. A common trend in the discussions was if an agency understands their enterprise capabilities prior to procuring a solution, they were better able to reduce their eventual Total Cost of Ownership (TCO), and transition to cloud computing faster.

The PMO asked agencies what initial considerations had the greatest long-term impact on their cloud adoption experience. Agencies emphasized the importance of four basic assets in the IT enterprise: network infrastructure, software licenses, identity management systems, and most critically, staff. Successful agencies started their cloud exploration with an assessment of their capacity in these areas and then used the findings to guide their path to the cloud. Agencies that overlooked these assets picked cloud solutions that did not fit their organizational needs and capabilities or, if providing services to other federal entities, those of their customers. These agencies subsequently faced a higher than expected TCO that ultimately made it harder to take advantage of expected cloud benefits.

Choosing a cloud solution that considers capabilities in these four areas does not guarantee success. Many stumbling blocks can halt an agency's progress, but this document will alert readers to challenges that agencies credit as the costliest and most damaging. These challenges are hazards which first-time cloud consumers tend to overlook due to their focus on the technical needs of a data center-to-cloud migration. This document will also highlight corresponding best practices other agencies have documented as key to their success. Good IT management practices enable agencies to save time and money re-configuring assets post-migration. Most importantly, better planning around these four assets will help an agency avoid being forced to return to a physical data center after an unsatisfactory foray into the cloud.

Scope

This document is not a definitive guide for moving to the cloud. Instead, it communicates to agencies lessons learned by their peers and the four recommended areas of initial focus most often cited by agencies.

This document is based on interviews with agencies that have used or provided one or more cloud solutions spanning the service model spectrum of Infrastructure as a Service (IaaS), Platform as a Service

(PaaS), and Software as a Service (SaaS).[1] The agency experiences and recommendations in this document are intended to be relevant regardless of whether an organization is using a private, public, or hybrid cloud deployment model.[2] Although this document is written to help agencies lower their future costs in any cloud environment, some stories and recommendations are more applicable to a particular service or deployment model.

Audience

This document targets three primary audiences: agencies that are currently or are interested in becoming cloud *Shared Service Providers (SSPs);* agencies that intend to be *customers of SSPs*; and agencies that want to be *customers of Cloud Service Providers (CSPs)*.

This document is based upon several assumptions about SSP and CSP customers. These agencies generally:

- Have already established a business case to move to the cloud;
- Are first-time cloud adopters and are currently in the discovery phase of their migration process;
- Have heard accounts from their peers about dissatisfying cloud experiences;
- Seek to understand the inputs that make up the cost of cloud computing. Their goal is to minimize their TCO; and
- Want actionable steps to identify and resolve enterprise capability gaps that will prevent a successful and cost-constrained migration.

This document is based on the assumptions that SSPs:

- Are currently providing cloud services (IaaS, PaaS, or SaaS) for another federal entity or have a formalized plan to offer such services in the future;
- Recognize a disconnect between the services they offer and the services their customers want;
- Seek more information about their customers' points of view on the challenges of procuring cloud solutions;
- Desire to lower their own TCO, and in turn, reduce the prices they charge customers; and
- Recognize current and potential customers have many service providers to choose from in the private and public sectors.

This document's intended audiences are agency and bureau Chief Information Officers or other high-level officials with management responsibilities in the cloud domain, from CFO Act and non-CFO Act agencies.

[1] "The NIST Definition of Cloud Computing." National Institute of Standards and Technology. September 2011. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[2] Ibid.

Background

M-16-19,[3] issued by the Office of Management and Budget in August of 2016, establishes the Data Center Optimization Initiative. This policy requires federal agencies to develop and report on data center strategies to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure. M-16-19 was the first codification of the federal government's Cloud First strategy[4] and the memo encourages agencies to use cloud infrastructure where possible when planning for new applications or consolidating existing ones.

The DCOI memo designates the General Services Administration (GSA) Office of Government-wide Policy (OGP) as the DCOI Managing Partner. In that role, OGP has conducted interviews with agencies that are investigating cloud solutions, agencies that plan to move data center resources to the cloud in response to DCOI, and agencies that have already made the move and struggled in the process. The Managing Partner offers guidance and resources to agencies through a series of topical white papers on cloud considerations, best practices, and innovations[5] that will help agencies comply with DCOI and the Cloud First strategy.

[3] "M-16-19: The Data Center Optimization Initiative." Office of Management and Budget. August 1, 2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf

[4] "Federal Cloud Computing Strategy." Office of the Federal Chief Information Officer. February 8, 2011. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

[5] For example: "IaaS Considerations for the Data Center Community." DCOI Managing Partner PMO, General Services Administration Office of Government-wide Policy. March 15, 2017. https://gsablogs.gsa.gov/gsablog/2017/06/14/how-to-be-cloud-smart/

Optimizing Network Infrastructure

Moving to the cloud is commonly seen as a logical exit strategy from the cost of maintaining an on-premises data center. However, multiple agencies encountered problems when they neglected to consider their outdated network infrastructure before orchestrating such a migration. The ability to access systems and applications hosted in the cloud is dependent on both an internal agency network and internet connection that can meet the bandwidth demands of cloud computing. If an internet connection cannot handle the exponentially greater volume of traffic that will be passing through it after a move to the cloud, optimizing the legacy network infrastructure is imperative. Otherwise, overburdened networks will at best increase response times and frustrate end users, and at worst make it impossible for an agency to feasibly run its applications and services in the cloud, forcing a return to the on-premises data center.

CSP Customer Experience

Despite having its network team's full support, a CSP customer struggled through its migration because of the critical roles played by external teams beyond its control. As a component of a larger agency, this federal entity needed the department-level network staff to help it navigate the agency's firewalls and other security configurations. Directing cloud traffic to the correct network endpoints in turn required obtaining accurate information from its CSP. The provider's DevOps process meant that the backend of the cloud solution was constantly changing, and the CSP's failure to communicate those changes meant that the federal component was often managing its connection to the cloud using outdated documentation. Until the component could successfully manage these relationships, its cloud solutions had recurring periods of downtime.

The difficulties that agencies experienced in accessing cloud-based enterprise services over a legacy network were commonly amplified by three particular complications. The first stemmed from the geographic distance created between hosted services and users, an inherent characteristic of cloud computing. After a move to the cloud, data typically must travel much further to reach an end user, increasing latency. On its own, this delay might be negligible, but when compounded by an outdated internal network infrastructure, it made the cloud unusable for some agencies.

The second roadblock to a seamless cloud experience faced by the majority of interviewed agencies is unique to the U.S. Federal Government: the obligation to route external internet traffic through a Trusted Internet Connection (TIC).[6] When the TIC initiative was established, applications and systems were typically hosted on-site, and this perimeter-based approach to defense did not impact access to these services. Because TIC requirements obligate federal agencies' internet traffic to move through a capped number of access points, it creates network bottlenecks which are exacerbated when a majority of users perform their day-to-day responsibilities with cloud solutions.

The third complication is a byproduct of the hierarchical structure of government agencies, which precluded federal entities from maintaining complete control over their network paths to the cloud. A single bureau or department's network is usually supported by switches, routers, firewalls, and TIC access points managed by multiple agency-level entities and private vendors. The adoption of one or

[6] "M-08-05: Implementation of Trusted Internet Connections (TIC)." Office of Management and Budget. November 20, 2007. https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2008/m08-05.pdf

more cloud solutions spreads the responsibility of maintaining critical pieces of that network among yet more providers. During a network-related cloud outage, agencies had to first determine the precise point of failure, and then identify the provider responsible for troubleshooting the problem.

If an agency can optimize its network before it moves to the cloud, it will successfully remove one of the major obstacles to a positive cloud experience, as well as one of the main drivers of an increased long-term total cost of cloud ownership.

Assess Network Capabilities and Needs

Agencies planning a move to the cloud should engage their network teams and all vendors supporting the network early on. These experts are needed to understand the existing network infrastructure in its entirety, including the various endpoints, security layers, and traffic flows. The division of responsibilities among the network teams and vendors should also be documented. Having a complete awareness of an organization's enterprise network structure is always a best practice, but it becomes critical when a substantial part of agency's business processes will be conducted using an internet or dedicated cloud connection.

CSP Customer Experience

One agency's expansive headquarters was unprepared for the bandwidth needs of cloud computing. Once an application that was formerly hosted on-premises was moved to the cloud, offices on the periphery of the campus experienced increased latency and reduced performance. This agency sought to make upgrades to its network infrastructure, including by procuring capabilities for higher internet bandwidth, to ensure optimal performance for all users in the organization.

All agencies, regardless of their existing network documentation, should map out their enterprise networks when they decide to move to the cloud. Many agencies which thought they knew their networks were surprised when they entered the discovery phase and found unknown endpoints or unexpected traffic patterns. Furthermore, a network that has been optimized to connect users to an on-premises data center will not likely be the best setup for connecting to a cloud-hosted IaaS, PaaS, or SaaS solution. Only if the network's specifics are fully understood can the necessary enhancements and fixes be made before a migration.

As part of the network discovery phase, an agency should also seek to understand its application requirements. Demand and usage patterns within the on-premises environment (particularly relating to data volume and flow) are predictors of the technical requirements for operating an application over the cloud. Using this information, an agency can perform a gap analysis between its current network capabilities and its expected bandwidth needs to determine what and where changes should be made.

Picking a Path

Agency interviews highlighted a few common methods for making a network cloud-ready. None of these methods are mutually exclusive, and some agencies implemented two or more. The choice of solution often depended on when in the migration process an agency discovered the shortcomings of its network

CSP Customer Experience

One agency expressed frustration with its cloud experience because the data transfer rates promised by its vendor did not materialize. This agency found that using the public internet, in combination with passing its data through the TIC, greatly reduced performance.

infrastructure. An organization that recognized the problem before the move could budget both time and money towards implementing the most efficient solution. An agency that discovered the issue post-migration, however, was sometimes forced to pick a less ideal but faster-to-implement fix to guarantee continued service availability.

Upgrade Internet Access

The most obvious solution for an obsolete network infrastructure that cannot meet the bandwidth demands of cloud computing is to upgrade the system with a higher-bandwidth internet connection. Network upgrades can be expensive and technically complicated, but if the new connection can handle future demand, the long-term costs associated with additional upgrades are limited.

Procure a Dedicated Connection

The roadblock caused by routing cloud traffic through a TIC access point can be avoided if an agency's CSP has dedicated connections available for purchase. A dedicated connection is a secure, private link that allows an agency's data to travel to and from its CSP without crossing the public internet. Agencies can independently procure a direct connection to their on-premises IT infrastructure, or take advantage of a co-location facility cloud exchange that offers direct links to multiple CSPs. An additional benefit of a dedicated connection is a more reliable network connection with reduced latency, as surges in internet traffic do not impact the private link. A major downside to a dedicated connection, however, is the associated costs. An agency must pay for its dedicated connection in addition to any data transfer fees that the CSP charges. Additionally, a dedicated connection can exclusively be used for cloud computing traffic, and thus an agency must also have an internet service provider for all non-cloud traffic.

SSP Experience

An agency encountered interrelated challenges when it tried to expand its cloud service offerings to its overseas offices. Many of these international sites had weak internet connections, which made them poor candidates for cloud computing in the absence of bandwidth upgrades. Slow performance was made worse when traffic had to return to the US to go through the TIC or to reach a US-based cloud solution.

Strategically Pick a CSP Hosting Location

Agencies can mitigate latency problems by strategically choosing between the cloud facilities run by their CSP or SSP. For example, an agency with a CSP that has several data center locations could choose to run its services out of the facility that was geographically closest to agency headquarters. However, this solution will not necessarily help users based in offices in other states or countries and may improve the cloud experience of one group of users at the expense of another group.

Move up the Stack

Based on the analysis of application requirements, in some cases it makes sense for an agency to move up the stack, away from its original intended cloud solution (e.g., going from an IaaS or PaaS to a SaaS solution). Similarly, obtaining a cloud-native solution designed to take advantage of cloud computing's scalability and automation capabilities is likely to require less bandwidth than continuing to run a legacy application that has been "lifted and shifted" into the cloud.

Optimizing the IT Workforce

Moving applications and systems to the cloud—even to a SaaS solution—does not eliminate the need for trained IT professionals within an agency. However, this shift does mean that the skills IT employees (both federal employees and contractors) need will be substantially augmented.

Federal regulations, contract language, and general HR logistics often make adding or removing workers within the federal government a prolonged process. As a result, an agency that decides to move to the cloud must immediately begin making plans about how to optimize its workforce to achieve success with its future cloud solution. The key task at this stage is for agencies to seek the best mix of current and new people who can provide the best value to the organization.

Agency Experiences

Cloud customers and providers recalled that staffing was one of the—if not the most—costly components of the cloud adoption experience. These agencies felt their workforces' expertise limited the extent of possibilities available to them in the cloud, but efforts to expand their staffing resources threatened to be financially excessive. Further constrained by regulations and policy, both consumers and providers lacked the flexibility to make easy and expeditious staffing decisions.

Provider Perspective

SSPs described struggling with their unique duty to recover their operating costs. This obligation forced them to have tough initial conversations about the expected costs and benefits of the different offerings they might provide. Multiple SSPs limited their cloud service provider selections to those with which their existing staff was most familiar, even before speaking with potential customers about their enterprise needs and staff abilities.

While these SSPs expressed satisfaction with their end products and felt they had successfully kept costs in check as much as possible, interviews with their customers revealed frustration that their provider was not listening to their needs.

SSP Experience

An SSP calculated that offering its solution with two underlying infrastructure options would be cost prohibitive because of the additional staffing costs it would impose. In its startup environment, this agency had a highly skilled team of developers with expertise and experience operating within a particular cloud IaaS. Offering a second version of its proposed solution built on an alternative IaaS would entail hiring a second team familiar with that system.

Customer Perspective

On the customer side, agencies grappled with moving to the cloud using an IT workforce that was well-versed in traditional data center operations. SSP and CSP customers who were most satisfied with their cloud experiences made the decision early to match a cloud solution to their existing data center staff assets. These agencies did not necessarily have the lowest ultimate cloud TCO, nor the highest cloud adoption rate of all interviewees. Rather, their high satisfaction rates stemmed from positive experiences in both the cloud migration process and the eventual permanent cloud environment.

These agencies did not have to undergo the burdensome process of hiring new employees because they selected solutions that fit their existing employees' skillsets. Consequently, there was no harm to workplace morale based on fear of job losses, and the time and money saved by avoiding the hiring process could be reallocated to the technical aspects of the migration.

Picking a Path

There are four primary ways that an agency can get its workforce cloud-ready and each requires varying amounts of time, funds, and other resources. The options listed below are ranked in order of lowest to highest cost (both financial and otherwise).

Option One: Match a Solution to Customer Needs and Abilities

Agency experiences show that matching internal staffing abilities to a cloud solution is not an ideal approach for providers unless they simultaneously account for customer requirements. Conversely, it is the preferred approach for first-time cloud adopters, as long as they have staff capable of managing a cloud solution that fits their general needs. A would-be SSP or CSP customer whose workforce does not possess any of the practical skills to manage a cloud solution is instead forced to choose between less ideal options for gaining the necessary capabilities.

Option Two: Train Existing Employees

When employees have little to no specialized knowledge needed in the cloud domain, an agency may choose to train its existing workforce. Providing staff with the opportunity to gain the skills needed to work within the cloud allows an organization to keep their employees' prior institutional knowledge. In a switch from a traditional data center to the cloud, employees who know an application's business domain can be invaluable.

In exchange for this knowledge, an agency must budget for initial training as well as retention bonuses that higher skilled employees may demand. Some vendors offer free training programs, but an agency should expect to dedicate part of its budget to general training and certification programs. The cost per person will depend on an employee's familiarity with need-to-know cloud tools. Cumulative costs will be highest if all or most staff require training not only on specialized instruction and possible certification in a particular cloud solution, but also in general cloud computing techniques (such as task automation and standard cloud management languages).

To avoid a higher than necessary TCO in the cloud, agencies should consider certain risks when deciding to retrain their existing staff. First, although training current employees is intended to be of service to the agency, there is the threat the newly-skilled individuals will be hired away by other organizations. Secondly, an agency still may have to reduce its workforce (e.g., because of budget limitations or fewer staffing requirements). Reductions can help an agency align with the long-term government obligations outlined in executive guidance issued in April 2017 within M-17-22,[7] but they will prompt the fears and resistance typical of a major transition.

[7] M-17-22: Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce. Executive Office of the President. April 12, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-22.pdf

Option Three: Augment the Workforce

Depending on the level of familiarity that existing staff have with cloud management techniques and specific solutions, it may make the most sense for an agency to fill knowledge gaps through the hiring or contracting processes. At a minimum, such an agency will need to procure a small team of cloud practitioners at different skill sets and salary levels. Even if an agency plans to have current staff support the migration, a single knowledgeable person cannot realistically orchestrate a major transition to the cloud. Although an agency should ideally have one individual responsible for championing the move and conducting a thorough and informed assessment of options, this person will need support from within the organization.

A staff augmentation risks being financially risky if it does not consider the cloud migration's expected outcome. Therefore, agencies must structure contracts and hiring agreements to reflect the reduced number and type of employees needed when they begin maintaining an established cloud environment. A contract, for instance, can allow the procurement of multiple labor categories. Failure to craft a long-term staffing strategy may force an organization to mold their migration workforce to fit the different needs of the post-migration environment.

For example, agencies pursuing IaaS or PaaS (and particularly those agencies planning on buying from a CSP) will require individuals with particularly specialized skillsets to guide their migration, such as cloud architects. Once the migration is complete and IT responsibilities shift more to DevOps and upkeep, they will not need as many of these experts. An agency that made no plans to offboard an expensive cloud architect might eventually need to assign that individual to lower-level maintenance tasks, something better upfront planning could have easily prevented.

Suboptimal staffing directly conflicts with M-17-22,[8] which instructs agencies to optimize their workforce, including how employee responsibilities are structured. As circumstances allow, the memorandum suggests reducing the number of higher-graded employees if a greater number of lower-graded (and thus lower salary) workers can reasonably perform some of their responsibilities.

Agencies will increase their likelihood of a lower TCO and chances of sustained success if they plan in advance for how they will make this staffing switch as their cloud environment matures. An optimized workforce also enables an SSP to pass on reduced costs to customers in the form of lower prices, helping to increase levels of customer satisfaction.

CSP Customer Experience

An agency saw a potential roadblock posed by its primarily-contractor workforce. Because this agency assessed its staffing assets very early in the cloud procurement process, it could have conversations with various on-contract vendors about the value they could add to the cloud migration. When a contractor did not offer or plan to offer services needed in the migration process and eventual cloud solution, this agency chose to let the contract expire–a tactic that was possible because it began staff optimization so early on.

Option Four: Retool the Workforce

In the worst-case scenario, existing staff will have no general cloud knowledge or domain-specific knowledge (e.g., if the on-premises applications are commodity IT). If an organization's

[8] M-17-22: Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce. Executive Office of the President. April 12, 2017. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-22.pdf

budget does not leave room to support both a physical data center IT team and a cloud IT team, an agency may consider retooling its IT workforce. Retooling would involve hiring new IT contractors and federal employees who are subject matter experts in cloud computing.

Some agencies have found retooling can save a significant amount of money. The efficiencies and automation capabilities in the cloud mean a lesser number of properly trained individuals can sometimes do the work performed by a larger staff in a traditional data center.[9] Even considering the premium tacked onto salaries for cloud experts, replacing ten traditionally-trained IT employees with three employees each earning twice as much will still save an agency 40% of prior salary costs.

However, a total workforce retooling may be more complicated in practice. Where contractors are concerned, it may not be financially prudent to break a vendor agreement. Waiting for a contract to expire, on the other hand, necessitates pushing back the target date for cloud adoption.

Staff optimization in agencies with higher proportions of federal employees can be equally difficult. An agency that is pursuing workforce reductions might prefer to repurpose existing federal employees rather than hire new ones. Agencies may find a seemingly simple solution of hiring cloud subject matter experts is not actually an option if budget limitations and organizational objectives prevent it.

[9] "Cloud Migration Business Analysis Guide." Draft, V 0.1.01. National Information Technology Center, USDA. https://community.max.gov/download/attachments/1237619918/Copy%20of%20Cloud%20Migration%20Business%20Analysis.pdf?api=v2 [Note: Accessible to individuals with a .gov or .mil email address only.]

Optimizing Identity, Credential, and Access Management Capabilities

As cloud adoption rates increase within the federal government, agencies will come to own or use multiple cloud solutions across IaaS, PaaS, and SaaS. Each solution needs to identify an authorized user and grant that user appropriate access rights. Once separate solutions are asked to work together in a hybrid environment, however, the process of implementing Identity, Credential, and Access Management (ICAM) becomes more complicated.

To provide a seamless cloud experience, every independent cloud environment must be capable of recognizing and validating the identities, credentials, and access rights provided by its counterparts. An inability to securely federate identities will force an agency to use inefficient and possibly risky alternatives. These alternatives will increase costs and negate the desired benefits of moving to the cloud.

Assess Enterprise Capabilities

In preparation for managing its workforce in the cloud, an agency should first fully assess their current ICAM capabilities. Any agency running applications and systems from a physical data center has some sort of ICAM process in place. Accounting for the features and limitations of this process enables an organization to later conduct a gap analysis to determine the changes required to make the existing setup cloud-ready. Alternatively, the gap analysis can help the organization decide which new solutions it must procure to be capable of administering effective ICAM in the cloud.

Federation

During the self-evaluation process, an agency should critically appraise the robustness of its enterprise ICAM capability. Above all, agencies must ask whether it includes the most basic ability to federate identities. The absence of an enterprise-wide identity federation capability is the foremost ICAM-related weakness agencies regret not remedying before migrating to the cloud because of the high cost to address it midstream.

Fault Tolerance

Organizations must also consider how fault tolerant their ICAM solution is, particularly if they plan to continue using it for cloud assets. The ability of users to connect to different cloud environments will depend on ICAM solutions being up, operational, and able to communicate with the other cloud solutions.

CSP Customer Experience

One CSP customer began considering its future ICAM needs in a cloud environment and sought to establish an internal identity federation competency long before it was ready to procure a specific solution. A representative noted that in hindsight, this early action was an especially critical factor in the agency's successful cloud migration. Its ICAM optimization process ended up delayed by several months due to internal bottlenecks, but because the agency started optimizing so far in advance, it could stay on track with its cloud migration timeline.

Security

Agencies seeking to move to a hybrid or public cloud should remember that in such an environment, security hinges less on the traditional perimeter approach to defense and more on the combined strength of many security subcomponents. What mechanisms does the current ICAM system have for preventing unauthorized access or stopping users from obtaining inappropriate permissions? If an individual does manage to get unauthorized access or permissions, how will the system identify and block the potential threat? The ability to federate identities is a requirement for interoperability among different cloud solutions, but it could also mean a security flaw will make the entire system vulnerable.

To prevent potential adversaries from taking advantage of the geographic flexibility cloud computing offers, agencies should tighten their ICAM security controls. Ideally, a system or application breach within a properly secured cloud will not guarantee access to confidential data. An assessment of existing ICAM-related security controls should include a thorough review of user permissions and data access rights. Agencies should remedy out-of-date or unnecessary permissions and restrict data to individuals who legitimately need it. An agency might further consider strengthening ICAM security through identity analytics, which analyzes user actions and alerts management to abnormal or inappropriate behavior.

Perform an ICAM Gap Analysis

The next step needed to position an agency to efficiently manage ICAM in the cloud is to perform a gap analysis of required products and competencies. This analysis should take into account the solutions discovered in the previous exercise that it does or does not want to continue using.
If an existing ICAM solution can be modified to work in the cloud, agency officials must consider the trade-off they would make by doing so. Using an already-owned solution saves the cost of purchasing a new one, but the agency must use resources to reconfigure it for the cloud. A cloud-native solution will be optimized for the new environment and may run more efficiently than an adapted data center solution, but it will involve a new procurement process and will likely incur additional costs.
Officials determining ICAM product needs must not overlook the front end, user-facing aspect of the cloud. Organizations want productive employees, and productivity will be hurt if users receive login prompts for every different cloud solution. To avoid this scenario, agencies need to acquire products that can integrate with enterprise federation and single sign-on solutions. These solutions should require support for Security Assertion Markup Language and OpenID Connect.

SSP Experience

A federal provider recalled that orchestrating a common ICAM system across multiple clouds proved surprisingly expensive, even though it was offering a limited number of solutions. This agency component was established specifically to serve as an SSP, and thus did not have existing on-premises identity management solutions to consider as it developed its policies and protocols. Nonetheless, establishing the ability to reuse identities between cloud-exclusive solutions required multiple products. This agency procured one product to manage its directory service in the cloud, and then used additional products to translate the directory service into the ability to identify users across the available cloud solutions. The agency had to budget for each of these products, which impacted the SSP's TCO as well as the prices that it passed on to its customers.

Address ICAM Gaps

Agency interviews highlighted the importance of determining the extent of ICAM needs as soon as possible to plan for funding and to allocate ample time to acquire suitable enterprise competencies and technology solutions. An agency that can take its time performing a gap analysis of current and required functionalities will be able to better consider its different options (i.e. modifying the current solution vs. procuring a new one). More time spent performing market research into potential ICAM solutions will help position an agency to make a cost-effective and suitable choice if it decides to make a purchase.

Addressing ICAM competency gaps early will also free up resources to prepare for managing ICAM when an agency's cloud portfolio grows. For example, an agency that is only starting procuring or offering a select few cloud solutions can plan how it will structure future contracts with vendors to ensure that identities can be federated between its new and existing cloud solutions.

Optimizing ICAM processes pre-migration is particularly important given the high costs of obtaining such an enterprise competency. Even under the best circumstances, developing an ICAM competency is markedly expensive, and the price will only rise if ICAM solutions must be reengineered to work with a cloud solution after the beginning of a migration.

Optimizing Licenses

Licenses primarily impact TCO in the cloud through the choice of licenses used and the approach by which those licenses are deployed across the cloud environment. Because any solution used in the cloud—regardless of whether it used as part of an IaaS, PaaS, or SaaS model—must be properly licensed, agencies can optimize their cloud experience by procuring and managing those licenses wisely. Agencies that reported being most successful at minimizing their TCO came to the early realization that they could no longer use the same approach to licenses that they did in their physical data centers. The unique characteristics of the cloud mean the mindset surrounding license ownership must change.

Conduct a License Inventory

A starting point for an agency interested in cloud computing is to inventory the licenses it already owns. To be valuable, this inventory must be more than just a tally, and a meaningful inventory will define the relevant characteristics of each license. This knowledge will help agencies eventually find a service compatible with its existing licenses, or acquire new licenses that enable it to work with the cloud service providers of choice.

License Allocation

At minimum, an agency needs to know the type of every license it has (i.e., perpetual vs. subscription based) and how they are allocated. License allocation varies by vendor and solution, and common allotment methods include a per-user basis, by enterprise usage, per CPU the vendor dedicates to the software, etc. Note that some of these allocation approaches may not translate well to the cloud, where the transitory nature of computing resources can prevent adding licenses to specific machines.

SSP Customer Experience

An inventory process highlighted the substantial number of duplicative software solutions used in an enterprise data center. Even before it explored how to most efficiently manage licenses in the cloud, this customer agency saved considerable money and IT staff hours by reducing the redundant software solutions it owned and maintained.

Licensed Tools and Products

An agency can lower its future TCO if it avoids migrating unused or unnecessary applications to the cloud. An inventory should therefore also capture the function performed by each licensed product and can coincide with a broader application rationalization process. Analyzing an agency's current licenses might reveal access to additional tools forgotten or underutilized at the enterprise level. Organizations often save money by purchasing software packages, rather than buying individual software licenses a la carte. These packages may include tools an agency initially did not use that may be useful in a cloud environment.

Understand the License Agreements

After surveying an agency's license portfolio, the permissions and restrictions defined in the various license agreements can be analyzed from a change management perspective. At this stage, an agency has not decided if it will use these same licenses in the cloud or if it will procure entirely new ones, and a thorough analysis will indicate how license agreements impact either scenario.

License Migration Considerations

In consideration of the possibility an agency will try to use a currently-owned license in the cloud, it should determine whether a vendor will honor an on-premises license, and, if so, what the approval process is. To budget properly, an agency needs to know if the vendor will charge a fee for using the license in a new environment, or if the move will impact the renewal price. Logistically, an agency must understand who will be responsible for orchestrating the migration. A further consideration is whether the licensed software is cloud-ready, especially if the agency hopes to migrate in a short time frame.

CSP Customer Experience

A representative recalled that an agency's migration could not commence until a vendor's data center application was cloud-ready. For that organization, the short-term cost of waiting was outweighed by the benefits of using software for which the enterprise was already licensed. Different agencies with different time and financial constraints may not come to the same conclusion, however, and may prioritize solutions that can be quickly adopted in the cloud.

License Abandonment Considerations

If an agency ultimately decides to procure new solutions for the cloud, it must know how much flexibility it has with existing licenses. If there are time constraints and an agency is determined to use a particular solution in the cloud, that agency may need to calculate whether it can afford to simultaneously pay for both the cloud version and the data center version of the product.

Picking a Path

Option 1: Map the Solution to Existing Licenses

Agency interviews revealed the popularity of basing their cloud solution choices off of their previously owned licenses. The most attractive aspect of this practice was the possibility of cost savings. In response to the demand for cloud computing capabilities, some vendors now provide licenses for cloud versions of their products with the purchase of a traditional desktop or server-based license. If an agency already has an enterprise agreement with a vendor, there may be no extra cost or a substantially discounted rate to use such a solution in the cloud. Although a different solution might be a better fit for an agency's functionality needs, this practice is in line with official guidance issued by the National Institute of Standards and Technology to "preserve existing investments in technologies which are appropriate to the cloud system."[10]

[10] "NIST Cloud Computing Standards Roadmap." *Special Publication 500-291, Version 2.* National Institute of Standards and Technology. July 2013. https://www.nist.gov/publications/nist-sp-500-291-nist-cloud-computing-standards-roadmap

The existence of enterprise-level licenses not only pushed customer agencies towards certain cloud solutions, but also steered them away from providers that did not support those solutions. Interviews with SSPs showed they understood customer agencies were often inclined to transfer on-premises licenses to the cloud. Yet customer agency representatives repeatedly described complications when an SSP was unable or unwilling to support a popular application or system in its service catalog.

SSP Customer Experience

An agency began the migration process only to discover that using its preferred system would involve paying for more servers and obtaining a new Authorization to Operate. The cost projection for using the system in the SSP's cloud environment promised to be so high that the agency hastily returned to a colocation data center.

Option 2: Buy New Licenses for the Cloud

Despite the potential cost savings of taking an existing enterprise license to the cloud, some organizations will have a business case for buying new licenses. Possible reasons include a desire to acquire a native cloud solution with no equivalent in a physical data center environment or dissatisfaction with current vendors. Organizations with no existing enterprise licenses for cloud-ready solutions will have no choice but to procure new licenses.

Agencies that are not tied to a particular product may find it most efficient to first pick a provider (or service to offer, in the case of an SSP), and then choose which solutions to use. The challenge with this approach is determining the product selection criteria and researching the many available solutions to find the best match. Agencies which successfully contained their TCO in the cloud recalled meticulously comparing the prices and functionalities of the solutions offered in their providers' service catalogs to those offered by third-party vendors. These agencies also purposefully looked for opportunities where commodity IT could meet their enterprise needs.

Whether an agency procures a solution directly from its provider or through an independent vendor on the market, it will ask many of the same questions that it did when procuring software for a physical data center. In particular, it will want to look at the contractual terms of a license agreement relating to price, length of commitment, ability to purchase or release additional licenses, etc. An agency choosing to use an external solution will need to verify that the provider accepts the license, and may inquire into any existing partnerships between the vendor and provider.

Upon choosing a solution, an agency must decide how many licenses it wants to purchase. This is a key factor in licensing costs that many agencies do not realize needs to be approached differently in the cloud. Although it was a best practice in a physical data center to purchase excess licenses to allow for growth, it is most cost-efficient in the cloud to target 100% utilization.[11] The flexibility of cloud computing means if more licenses are needed, procuring them is a quick and straightforward process. For example, a temporary need for additional licenses can be remedied in an IaaS environment by purchasing instances with bundled licenses (see "Bundled Licenses" below). Organizations that over-provisioned licenses in the cloud ultimately had a higher TCO, while agencies which recognized this shift had better control over costs.

[11] Providers licensing solutions to offer customers can be the exception to this rule: one SSP found that it saved money by buying substantially more seats than it needed to obtain a volume discount.

Agencies that want a new solution for the cloud without the complexities of the license procurement process might consider acquiring a SaaS solution. Since the service in SaaS is for the software product itself, the customer usually has access to a simplified license management framework.

Provider-specific Considerations

An SSP should ensure customers can use the same funding source to pay for new cloud licenses and support services as was used for on-premises licenses. For example, some federal agencies pay for their data center software licenses through an agency-funded working capital fund. If an SSP does not accept money from this working capital fund, the entity will need to find another source of financing (e.g., its internal component budget) to procure cloud services. The SSP will consequently *appear* to be the more expensive—and less attractive—option in comparison to remaining in a physical data center.

Deploy Licenses

Unlike traditional computing in a physical data center, cloud computing is not tied to a static array of hardware infrastructure. Customer and provider agencies had to grapple with the question of how to allocate and manage licenses when the operating systems running cloud solutions could move within different provider-managed data centers, across state or national lines, and between cloud environments operated by different CSPs or SSPs.

This was particularly challenging in an IaaS environment, where agencies could auto-provision an indefinite number of new servers. The management tactic which most successfully reduced IaaS license costs was the recognition of two main approaches to license deployment in the cloud. A combination of these deployment models could fully meet an agency's needs while minimizing inefficiency and waste.

Bring Your Own License

In a steady-state environment where a consistent level of demand is placed on compute resources, the Bring Your Own License (BYOL) approach is best for reducing an agency's TCO. BYOL involves installing previously purchased licenses on every provisioned instance. Provided that controls are in place to prevent the automated generation of additional virtual servers, BYOL lets an agency cap the number of licenses it pays for in any given period, which can help with IT budgeting.

Bundled Licenses

Agencies which periodically need to auto-scale new instances to meet increased demand should purchase instances with licenses included, or bundled, in the virtual server. Instances with on-demand licenses cost more than instances without them, but they mitigate the risk of an agency spinning up more servers than it has licenses. The terms of a license agreement may require an agency to pay the full license cost in such a scenario, even if it is only used briefly on a temporary instance. An additional benefit of using an instance with bundled licenses is that, like SaaS, license compliance is the responsibility of the SSP rather than the customer.

Conclusions

Much of the cloud's appeal comes from the ease with which organizations can add new capabilities to their service environment. The installation of new solutions may take as little as activating a tool already offered by a provider or third-party vendor and making any necessary configurations. This ease is markedly different from the technically complicated hardware and software installation processes required in a physical data center.

A common misconception is that when organizations migrate to the cloud, any additional changes to the environment are effortless. In reality, organizations have far less flexibility in regards to network infrastructure, human capital, licenses, and identity management systems than they do with technology-centric elements of a cloud environment. It takes more time, funds, and other resources to make changes to these four assets, particularly after a cloud migration is complete.

As some agencies' experiences prove, initial strategic planning helps an agency reduce the need to course correct midstream. An organization can avoid delays and out-of-control costs by fully considering these areas before investing in a cloud service or solution. An agency that stays on schedule, in scope, and within budget will ultimately have a lower TCO and overall greater satisfaction with its cloud service. These successful cloud migrations can serve as models and encourage further agency-wide adoption of cloud computing solutions.

For more information about this white paper, data center shared services, or cloud-based services in general, contact the DCOI Managing Partner PMO at: dcoi@gsa.gov. The DCOI Community of Practice (CoP) also provides meeting materials and a link to a more detailed knowledge portal. Anyone with a ".gov" or ".mil" email address may access the CoP using the MAX Federal Community at: https://community.max.gov/x/DI5tQw.

Appendix A: Suggested Resources for the Federal Government

GSA-Based Resources

- Cloud Blanket Purchase Agreements - https://www.gsa.gov/technology/technology-purchasing-programs/cloud-blanket-purchase-agreements-bpas
- FedRAMP Key Cloud Service Provider Documents - https://www.fedramp.gov/resources/documents-2016/
- FedRAMP Key Agency Documents - https://www.fedramp.gov/resources/documents-2016/
- FICAM Community of Practice - https://www.idmanagement.gov/community/
- FICAM Playbooks - https://www.idmanagement.gov/build/#playbooks
- ITCSC Cloud SOO Templates - https://www.gsa.gov/technology/technology-products-services/cloud-computing-services/cloud-soo-templates
- Office of Federal Procurement Policy's Federal Acquisition Institute - https://www.fai.gov/drupal/

Government-wide Resources

- CIO Workforce Committee - https://www.cio.gov/about/committees-affliates/workforce-committee/
- NASA Solutions for Enterprise-Wide Procurement - https://www.sewp.nasa.gov/
- NIST Cloud Computing Collaboration Site - http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/WebHome
- NIST Cloud Computing Program - https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp
- NIST SP 800-63 Digital Identity Guidelines - https://pages.nist.gov/800-63-3/
- OpenID Connect - http://openid.net/connect/
- Trusted Internet Connections (TIC) Reference Architecture Document - https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf

Vendor-Neutral Resources

- ACT-IACT Cloud Community of Interest - https://www.actiac.org/cloud-community-interest
- Cloud Security Alliance - https://cloudsecurityalliance.org/
- The Advanced Technology Academic Research Center Cloud & Data Center Working Group - https://www.atarc.org/working-groups/cloud/