Data Center
Optimization Initiative

# CLOUD READINESS

## Preparing Your Agency for Migration

**APRIL 18, 2018**

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

# Cloud Readiness:
# Preparing Your Agency for Migration

## Purpose

This white paper outlines the topics and processes agency Office of the Chief Information Officer (OCIO) leadership should consider when preparing for a data center migration to the cloud. This paper will not cover every facet of cloud migration readiness, nor is it a how-to guide on cloud migration alone. Instead, it highlights key considerations for agencies as they prepare to migrate to the cloud, what risks may arise when preparing to migrate, and possible ways to mitigate those risks.

If an agency's cloud readiness assessment incorporates many of topics highlighted below, it will be flexible enough to handle unexpected obstacles while remaining cost and time efficient. Regardless of whether an agency decides to engage with a vendor or conduct a migration alone, agencies should consider these steps and topics in preparing for an assessment since they are fundamental in understanding how agencies can utilize cloud for their IT services.

This whitepaper supports the Office of Management and Budget (OMB) Memorandum M-16-19 "Data Center Optimization Initiative (DCOI)," dated August 1, 2016.[1] Additionally, this document is aligned with the "Cloud First" strategy, and seeks to aid agencies in planning a move to the cloud.[2]

## Audience

The intended audiences of this paper are agency CIO offices, project management teams, data center operations teams, and data center migration teams at both the physical source and destination in the cloud environment.

## Aligning Resources and Building Capacity

Migrating to the cloud is a massive undertaking that involves many stakeholders throughout an agency. Agencies must be deliberate in marshalling their resources to prepare for this endeavor while simultaneously building capacity within their ranks. Building capacity should include developing technical cloud skills among staff or instituting new accounting procedures for paying cloud providers. Agencies should focus on the following areas in preparing for a cloud migration:

- Cloud strategy;
- Security needs;
- Enterprise-wide inventories;

[1] See: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_19_1.pdf.
[2] See: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

- Change management;
- Workforce factors;
- Financial considerations;
- Internal resources;
- Data needs;
- Network topology; and
- Cloud management platforms.

## Cloud Strategy

With the adoption of the "Cloud First" strategy, agencies must consider cloud computing options as part of their technology strategies. In doing so, agencies should identify their mission priorities and examine why migrating to the cloud supports those priorities. While the cloud can provide a range of services and benefits, it may not be applicable to all the needs of an agency. For example, an agency seeking to migrate may possess a large proportion of necessary infrastructure that cannot easily be migrated because of geographical limitations. In that case, an agency might consider adopting a colocation service model instead of utilizing a cloud service provider (CSP) since colocation can allow an agency to use its legacy infrastructure without being fully responsible for maintaining that infrastructure.

Agencies should identify the specific benefits they seek to gain from the cloud, such as increased application availability and provisioning on-demand services, and map those benefits and services out within the agency, essentially building a business case for the cloud. Furthermore, agencies should identify the types of cloud cost savings relevant to their mission. Clarifying what an agency wants from the cloud will guide stakeholders and help the agency in properly scoping its migration strategy.

## Security Needs

Agencies should determine their data security needs and how the cloud can serve them. Security is sometimes cited as concern among agency staff when thinking about migrating. While many believe that the cloud is less secure than physical data centers, cloud services and facilities typically possess the proper security architecture and certifications to provide services for the government. Many cloud providers are FedRAMP and Federal Information Security Management Act (FISMA) compliant and can tailor their services to meet the specific security needs of federal clients. Identifying an agency's security needs assists policymakers in properly scoping the agency's migration strategy. Additionally, as data centers migrate to the cloud, agencies can limit their potential attack vectors by decreasing the number of physical data centers. Vendors can often offer more physical security for their data centers when compared to unsecured server closets or rooms. Finally, vendors can also supply cloud computing services, like cloud cross-connections, within the spectrum of tier classifications, from Tier I to Tier IV, providing increased redundancy and disaster recovery capabilities.

## Enterprise-wide Inventories

Before an agency begins the migration process, it must fully understand the networks, systems, and applications that comprise the IT infrastructure. Therefore, agencies should perform an enterprise-wide inventory of their IT infrastructure, especially of infrastructure that may be migrated. For example, conducting a network inventory allows agencies to acquire a better understanding of their data bandwidth requirements across the enterprise footprint. This information is helpful in determining the data specifications of any cloud environment agencies want to migrate into.[3] One of the most common complaints from vendors is that when they work with government agencies on cloud migration, those agencies frequently lacked enough knowledge of their own infrastructure. This has resulted in vendors spending more time and resources performing an inventory, delaying the entire project and increasing costs. While many vendors have the capacity to perform inventories, agencies should not assume that vendors can quickly shift focus and perform an inventory without incurring costs or delays. Performing an inventory will also guide agencies as they determine what sort of cloud models and services may best fit their business needs. Before any vendor is engaged, agencies should take the time to complete a detailed discovery process. Doing so will help identify which applications and systems are suitable for cloud migration.[4]

*Agency Experience*

*One agency recounted how staff apprehension of migrating to the cloud, based partially on fears of losing job security, led to friction between the agency leadership and staff. To rectify this, the leadership developed ways to train up their staff in the new technology and clearly show where they fit in the new structures. The agency's vendor, which had already been contracted to assist in migration, was brought in to conduct free seminars designed to answer a vast majority of the staff's questions. These steps not only brought the staff on board with the cloud migration, but also provided the agency with a deep bench of staff with technical skills needed to service the cloud. Furthermore, the agency was able to retain most of their staff afterwards.*

## Change Management

Agencies should establish a change management strategy to successfully migrate to the cloud and identify the staff needed for implementation. Managing a smooth transition and developing ways to handle challenges that may arise during the migration process are two key aspects of any successful strategy. For example, staff at current data centers may believe that, as the migration to the cloud continues, they will lose job security due to greater efficiency or a lack of a technical knowledge base to maintain the new cloud environment. Agency leadership can bring staff on board by addressing staff inquiries and concerns directly. For example, leadership may bring in cloud vendors to explain the

[3] See "DCOI Guide for Data Center Migration, Consolidation, and Closure" for more information on how to conduct a detailed discovery of an agency's applications and systems: https://www.gsa.gov/node/95396.
[4] See "DCOI Guide for Data Center Migration, Consolidation, and Closure" for more information on how to conduct a detailed discovery of an agency's applications and systems: https://www.gsa.gov/node/95396.

security strengths of cloud services, provide training to build capacity, and emphasize that staff can remain relevant despite the changing environment. Leadership can highlight how staff will fit into the future state and frame cloud migration as an opportunity for staff to gain a new set of skills.

Alternatively, as staff develop new skills to service the new cloud environment, agencies should develop ways to manage staff attrition, especially after staff gain new skills. While staff attrition is a commonplace occurrence, gaining new cloud skills could make staff more likely to leave federal service. For example, some staff may opt to leave agencies instead of being re-trained. Without a proper knowledge transfer, the agencies may lose significant domain knowledge as staff, both federal and contractors, leave federal service.

*Accountability Guide*

*One artifact agencies should consider creating is an accountability guide. This guide outlines who in the agency is responsible for a specific function, process, or area of focus in terms of a cloud migration. The guide should include the contact information for each individual. Creating such a document can serve multiple purposes. Not only can this guide help agencies identify key stakeholders internally, it can help vendors who are contracted to help in migration. This guide can also ease the onboarding process of any new stakeholders or support included in this process.*

Agencies should also consider which staff should be included in cloud migration teams. These teams will lead the migration effort and will act as the primary point of contact with any vendors assigned to assist in the readiness and migration process. Establishing migration teams with clear responsibilities and mandates (e.g., procurement, cybersecurity, data transfer) and assigning motivated people to the right teams can ease the adoption of a migration strategy. As a result, an agency will have units with a singular focus on specific migration tasks with the flexibility and capacity to handle tasks and challenges as they appear. Relying on ad hoc processes can become an obstacle in migration as the scale, speed, and complexity increase. Agencies that create specific and detailed processes are better positioned to control costs and save time.

## Workforce Factors

As agencies adopt cloud platforms and related technologies, they should ensure that their staff has the skills necessary to transition to working in the cloud environment. Specifically, as part of their cloud readiness strategy, agencies should:

1. Identify their cloud skill needs beyond cybersecurity considerations; and
2. Demonstrate how they will retain, recruit, and reskill staff with these necessary skills.[5]

Existing staff may lack the skills or knowledge required to facilitate a cloud migration effort or to maintain the environment once migration is complete. For example, operations staff may not be able to shift their thinking from servers and storage to orchestrated services, development staff may lack experience in making the cloud environment work, and acquisition staff may lack understanding of the

[5] See "Staffing" in the "Key Cost Considerations for Agencies Planning Cloud Migrations" for more information on handling staff issues, see: https://cioknowledge.max.gov/?q=node-detail/1109247 [Artifact only available to those with government email accounts].

differences in various cloud service offerings. Staff working in traditional IT infrastructure may be responsible for functions such as server backups or disaster recovery and continuity of operations which are managed differently in a cloud environment than in an on-premise one. Moreover, creating new applications and migrating old ones will often require new skills and knowledge of containerization and virtualization, microservices, self-healing systems, continuous integration and development, and other modern techniques. Although members of the government team may not be undertaking the work directly, they will need to be deeply familiar with these topics to both acquire and manage vendors and contractors effectively.

While anticipation of every staffing need brought by cloud adoption is difficult, agencies should map out potential personnel and cultural impacts of migrating to the cloud before migration occurs. The workforce needs of operating in the cloud will extend beyond cybersecurity skills, such as providing training to non-technical staff as they transition to new support positions. Agencies typically focus too narrowly on the IT workforce impacts of cloud because agencies themselves often do not realize how on-premise data centers impact the wider workforce. Agencies may inadvertently overlook non-technical staff at on-premise data centers when planning migrations and therefore are unprepared to assist non-technical staff when the migration strategy is implemented. For example, if moving to the cloud will lead to a reduction in on-premise data centers, agencies should develop contingency plans for maintenance or security staff who may be impacted, ranging from reassigning those staff members to providing training in their new area of focus as part of the cloud team. Agencies should also recognize that moving to cloud may reduce the workload for certain non-cybersecurity staff. For example, human resources personnel who work with on-premise data centers may experience a lighter workload since there would be fewer on-premise staff to support.

Leadership must address how moving to the cloud will impact non-cybersecurity personnel as part of a risk mitigation strategy by identifying obstacles associated with the current change culture and personnel management. One crucial way to address staff resistance is to communicate the vision for the organization that the migration will achieve, the changes that will take place for the migration to be implemented, and how staff will play a part in this vision through adaptation of roles and skills. Enabling staff to provide feedback on the vision and the changes, as well as help develop the migration effort will enable buy-in to the overall plan and increase successful participation in training and career shifting to cloud-focused or support roles.

Below is a non-exhaustive list of examples of non-cybersecurity staff that may be impacted when agencies migrate:

- Physical maintenance crews (e.g. HVAC maintenance);
- Physical security (e.g. security guards at on-premise data centers);
- Administrative staff;
- Janitorial crews at on-premise data centers;
- Human resources; and
- Acquisition staff who cover on-premise data centers.

To mitigate the skill and knowledge gaps in the current workforce, agencies should maintain an up-to-date list of the skills of current staff and a separate "dream team" list of positions and skills needed in the new cloud environment.[6] Agencies can inventory the skills and expertise of current staff to identify strengths, weaknesses, and opportunities within the current workforce. This inventory could account for certifications and trainings staff have completed along with proven technical track records, such as experience working with specific cloud platforms or technologies. Agencies should also perform an inventory of position descriptions and contracts to make sure that they are seeking the proper skills from contract support or from potential new agency FTEs, and determine how current staff fare when compared to the wider IT workforce through benchmarking. In anticipation of training staff, agencies should also evaluate the training budget and ensure that it is flexible enough to provide for the needed training to fill the identified skills gap, either by a vendor or by the agency itself. Agencies should also identify potential opportunities to incentivize re-skilling when possible, such as contracting a vendor to provide training seminars during migration.

## Financial Considerations

Agencies must develop financial mechanisms to map out and pay for the costs of migration. The pre-migration optimization of enterprise capabilities (such as staff and network infrastructure) is intended to lower an agency's ultimate total cost of cloud ownership.[7] Migrations frequently lead to costs ranging from testing applications in the cloud environment to procuring new technology. Agencies can position themselves ahead of problems like cost overruns due to testing or technical capacity building by developing financial structures that are flexible enough to address those costs when they arise. Agencies should create teams to address these financial issues related to moving to the cloud. In turn, the teams should develop accounting procedures needed for migration, and financial structures flexible enough to address shifting costs.

Because cloud computing allows agencies to treat IT as operating expenses (OpEx) rather than capital expenses (CapEx), agencies should consider the financial trade-offs of moving towards a more OpEx-focused model from a CapEx model. The cloud allows agencies to provision services (like the number of virtual machines needed to fulfill a customer's request) in the cloud as needed. Instead of purchasing assets for long term use, agencies should adopt accounting procedures to ease in transitioning into an OpEx model. New measures agencies can consider in an OpEx model include paying vendors on a monthly basis instead of upfront or listing operational expenses as operating costs instead of depreciation. The IT governance at any agency migrating to the cloud needs to adapt to this change in perspective. Staff involved with purchasing and budgeting IT services may require training and assistance in easing into an OpEx model.[8] This is both a financial and organizational challenge for

[6] The DCOI PMO will be releasing more information about the skills and positions required for a cloud "Dream Team" in a future paper.
[7] See "Key Cost Considerations for Agencies Planning on Cloud Migrations" for more information on how to conduct a detailed discovery of an agency's applications and systems, see: https://cioknowledge.max.gov/?q=node-detail/1109247 [Artifact only available to those with government email accounts].
[8] See "IaaS Considerations for the Data Center Community" for more information on how agency leadership can provide surge funding for staff trainings: https://www.gsa.gov/cdnstatic/white_paper.pdf.

agencies as they prepare to move to the cloud.

## Internal Resources

Throughout the planning process, agencies should include employees that have unique perspectives on migrating to the cloud, such as those involved in data center optimization management. These employees could include data center managers, facility managers, and whoever is tasked with leading an agency's data center optimization initiatives. These individuals possess unique skill sets, have deep institutional knowledge of an agency's data centers, and can tap into networks that can supplement the knowledge required to lay the foundation for a successful migration. Furthermore, these employees can act as points of contact for any contractors that are brought in to assist in migration, especially during the inventory phase.

## Achieving Success

While the aforementioned topics are not an exhaustive list, agencies that are able to apply these principles are more likely to develop a successful migration strategy while avoiding many of the typical stumbling blocks other agencies have encountered. Additionally, agencies will have a better understanding of what to ask for from potential vendors, thus ensuring that vendors are better positioned to provide the needed services.

*Agency Experience*

*An agency undergoing a migration brought a smaller vendor on board for assistance. While the vendor was able to provide a variety of services ranging from business strategy to staff trainings, because other groups within the agency were not prepared for migration, the agency ended up only taking advantage of a slice of the vendor's offering, missing out on major benefits. Agencies should be deliberate in mapping what services they want from a vendor and build up capacity to take advantage of the offerings of a vendor.*

# How to Engage with a Cloud Readiness Vendor

Frequently, agencies will rely on vendors for assistance in cloud readiness.[9] Vendors can enhance the agency's plans and strategies by providing previous experience and capacity. While the spectrum of vendors varies from small to large, the types of core services that cloud readiness assessment vendors provide are common industry-wide, as noted in the previous section.

Agencies should perform market research on cloud readiness assessment vendors prior to engagement. Many vendors provide online pre-assessment tools or provide one-day seminars highlighting their services. When agencies perform market research prior to engagement, not only will agencies have a better understanding of the services available but market research that will help agencies in determining

[9] For more information on how to engage with professional vendors in the cloud space, please review the Cloud Special Item Number (SIN) 132-40: https://www.gsa.gov/technology/technology-purchasing-programs/it-schedule-70/sins-and-solutions-we-offer/cloud-special-item-number-sin-13240#listings.

what they ultimately want from vendors.

While the type of vendor agencies ultimately engage with will depend on the business needs, agencies are encouraged to join the DCOI Community of Practice (CoP) to share best practices on how to engage a vendor or to engage with General Services Administration (GSA) resources to help with issues such as procurement. Instructions on how to join the DCOI CoP are at the end of this paper.

## What to Look for in a Vendor

Vendors can provide an agency with technical expertise, technology solutions like cloud management tools, and staff training, like educating employees on the merits of lift-and-shift or cloud native delivery methods. Vendors range from large companies that can provide both migration services and their own cloud products, to smaller firms that focus on preparing agencies for migration. These smaller firms may partner with a large cloud service provider. While the type of vendor an agency ultimately enlists will depend on its own circumstances, there are several common themes an agency should consider when searching for a vendor. The following, although not exhaustive, should be included in any criteria when selecting a vendor:

- A proven track record of successful migrations, including the number of cloud readiness assessments completed in the past (including federal migrations);
- Technical expertise and customer support as seen by cloud certifications;
- Security certifications;
- Partnerships with CSPs;
- Application and systems inventory support;
- Post-migration support, including but not limited to enterprise architecture;
- Experience with federal clients;
- Availability of training to build up staff cloud capabilities; and
- Which services the vendor will provide in-person and on-site versus remotely.

## Core Vendor Services

The core services provided by cloud readiness vendors can be bucketed into three groups: assessment, strategy, and migration.

**Assessment** focuses on working closely with a client to lay the foundation for a successful migration. This step determines the capability of an agency to migrate to the cloud based on the people, processes, and systems within that agency. It is during the assessment stage that a vendor may either conduct an inventory or assist the agency in doing one. During this phase, vendors will frequently investigate an agency's network performance, server infrastructure, and applications as well as the suitability of the agency's services or workloads in the cloud space. Vendors can also assist agencies in developing a methodology to determine what applications are cloud ready at this stage.

Vendors will also typically determine how the transition will affect the agency's mission or support

services. Some vendors construct a business case for the agency to determine what type of cloud model or service best suits the agency, or to validate the agency's choice of cloud environment in light of its business needs. Vendors may differ on how to conduct the assessment, with some preferring to be present on-site while others performing the assessment remotely. If agencies prefer a vendor to be onsite, agencies should consider travel costs in any contract anagency enters, especially if the vendor needs to travel to specific locations or data centers.

Next, vendors will develop the **strategy** for migration in cooperation with their client. At this point, the agency and the vendor will have a better understanding of which applications and systems will be moving to cloud. Vendors may take this opportunity to perform a more comprehensive assessment of mission-critical or legacy applications or systems that require more attention in preparing for migration. Vendors are likely to test an agency's applications in the cloud space. Vendors that do not include building a business case in the assessment stage will do so in this step. Discussions about what type of cloud service and delivery model an agency should adopt tend to occur in this stage as vendors provide agencies with their recommendation based on the inventory, application tests, and business strategy. The roadmap or strategy developed between a vendor and agency should be a living document, allowing both actors to adapt the strategy in light of new developments during the migration process.

With the assessment and strategy developed, vendors enter the last stage: **migration**. With a comprehensive understanding of applications and systems and a strategy developed, vendors will initiate the migration. This step includes developing business continuity options and determining a migration schedule for the targeted applications and systems. Both groups should also map out any post-migration services the vendor will provide, such as the tools the vendor will provide to monitor the applications in the new environment.[10]

## Vendor Services Delivery Methods

Vendors vary in how they deliver their services to their clients. Services can range from daily, hands-on guidance and monitoring to remote online assessment tools that agencies utilize on their own. The range of services allows agencies to act more selectively in the types of delivery methods they choose. Most vendors produce online prospectuses that generally outline their delivery methods. Fundamentally, the type of delivery method agencies chose should be informed by their cloud needs and available resources. For example, if agencies decide to enlist vendors that only provide onsite services, agencies must account for any time or costs associated with provided security clearances and any facility accommodations needed, like desks or office space for the vendors. Delivery methods range from manually migrating data between the new and old environments to full server failovers into the cloud. Agencies should consider the delivery methods vendors provide when conducting market research. Doing so should narrow the universe of vendors agencies can consider if certain delivery methods are incompatible for certain agencies.

[10] See "DCOI Guide for Data Center Migration, Consolidation, and Closure" for more information on the migration process and timelines: https://www.gsa.gov/node/95396.

## How are Vendors Different?

While there are many vendors in the cloud readiness space that share core services, there are key distinctions between the types of vendors that may influence which vendor is ultimately chosen. Ordinarily, vendors differ in both specialization and size. Cloud readiness vendor specialization can be divided between two types: those who focus specifically on readiness strategy, and CSPs who also offer readiness services. The first category of vendors partners with one of the major CSPs and specialize in migrating to that specific cloud service. These vendors can provide expansive knowledge of a particular cloud service, although they may not have the same expansive knowledge set for other cloud services. Some further specialize by only providing readiness services without helping a client migrate to a specific cloud environment. These vendors may have extensive experience in providing inventory services and building business cases but do not go further. Sometimes these vendors are also customers of cloud services themselves, potentially providing another perspective that federal clients can take advantage of. Vendors that are also CSPs not only have a massive network to tap into for expertise and technical support but can also streamline the entire cloud adoption process since the readiness, migration, and destination phases are all kept in-house. They can also provide services from start to finish, from the assessment phase to post-migration phase. However, agencies may not have an easy time in trying out other CSPs if they opt to bring on board a vendor that is also a CSP, and can become locked into a specific solution or contract. Some CSPs do offer mapping services that can scan agencies' data centers for purchase, provided that necessary security precautions are taken.

Vendors also come in various sizes, ranging from the boutique firms to large multinational corporations. While the size of the vendor does not necessarily impact the type of services provided, it can impact the degree or the breadth of services. For example, vendors are frequently enlisted to train staff on the new skills needed to maintain the cloud. Smaller vendors may not have the capacity to train all the staff at large agencies. Larger vendors, on the other hand, may not have the bandwidth to provide constant customer engagement with an agency the way a smaller vendor might. Deciding which type of vendor to engage with ultimately should be determined by the types of services agencies need, vendor size notwithstanding. Both larger and smaller vendors each have their own strengths and weaknesses, including factors such as the ability to bundle services, agility, and specialization. As such, the step of soliciting information from and selecting vendors is one of the more crucial in the cloud migration process.

Regardless of the type of vendor an agency ultimately chooses, any request for work or information must include clear requirements specific to a cloud readiness assessment. This will help vendors self-select and will avoid delays and cost overruns in the future. For example, vendors may be brought on to assist on a cloud readiness assessment, only to discover that there is a dire need for an enterprise-wide IT inventory. While these vendors may have the capacity and expertise to conduct an inventory, the overall project may be delayed with growing costs since the vendor needs to halt any progress and run an inventory for their client before moving forward. When clients clearly state in the work order that they want a vendor to do an inventory in addition to helping with other aspects of cloud

readiness, they can save time and money. The vendor can adequately prepare itself to conduct the inventory and align its own resources to address that task. Thus, clients whose requests for work or information have clear requirements avoid having to wait while vendors reorient themselves to conduct an unanticipated inventory, avoiding major delays.[11]

## Conclusions

Cloud readiness assessments are an integral part of any cloud migration strategy. Agencies that take the time to identify what exactly they want from the cloud in addition to understanding the breadth of their own capabilities will position themselves for success. Spending time on the front end to map out a strategy and formalize processes will save time and control costs in the future.

For more information about cloud readiness contact the DCOI Managing Partner PMO at: dcoi@gsa.gov. The DCOI 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.

[11] See "Creating Effective Cloud Computing Contracts for the Federal Government" for more information and guidance on how to effectively procure cloud services. https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.