Data Centers
Shared Solutions Marketplace

IaaS Considerations for the Data Center Community

DCOI PMO Cloud Series

Version 1.11
March 15, 2017

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

IaaS Considerations for the Data Center Community

Purpose

This whitepaper from the Data Center Optimization Initiative (DCOI) PMO,[1] shares some of those lessons learned to provide a holistic view of cloud adoption and enable the federal data center community to be "cloud smart."

Background

The OMB DCOI Memo M-16-19 directs federal agencies to consider the cloud first when evaluating data center closures and optimizations.[2] Under the "Cloud First" strategy,[3] numerous federal agencies have moved operations to the cloud and shared their success stories and lessons learned via workshops, seminars, and conferences.

The DCOI PMO is dedicated to ensuring that our client agencies are provided relevant information and are directed to proper resources in regards to organizational cloud transformations. Please contact us at dcoi@gsa.gov to improve this publication or learn more about federal cloud implementation resources and solutions.

Any reference of an Infrastructure as a Service (IaaS) provider is not to be considered an endorsement of that provider, but is meant to provide further illustration of a presented concept.

Business Drivers

The DCOI Memo indicates that agencies should evaluate cloud technologies first in closing and consolidating data centers. This section covers a few areas which should be included in the business justification for a cloud transformation.

Cost

Many IT leaders say that the number one business driver for migrating to the cloud is a better Return on Investment (ROI), but it can be difficult to validate ROI if the current environment is not already priced out at service levels. In addition, organizations may not receive a positive ROI in the initial years of a

[1] The DCOI PMO is the managing partner of the Federal Government's data center line of business and data center shared services.
[2] M-16-19. Data Center Optimization Initiative. 8/1/2016. https://policy.cio.gov/dcoi/
[3] As articulated in the Federal Cloud Computing Strategy. 2/8/2011.
https://obamawhitehouse.archives.gov//sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf

cloud migration, because of the migration costs and any realized cost savings may be a result of the process of pruning inefficiencies during migration, rather than the cloud technology itself.

In the absence of clear service level pricing, the decision to migrate to a cloud environment should include a business need requiring IT flexibility. Since many federal entities will not delve into non-FedRAMP'd cloud services, major flexibility is often not realized out-of-the-box, because the Federal Government does not always leverage all available opportunities (such as where underused resources are sold to the highest bidder).

Application Modernization

A cloud migration provides an opportunity for IT portfolio consolidation and application rationalization as part of a cloud readiness assessment. Application owners can evaluate the usefulness (how often is each system used, and is it even aligned with the business anymore?) and repetitiveness of functionality (are several systems performing the same function across the enterprise?) in the application layer. This evaluation can help to determine what should be ported to IaaS, as well as what should be consolidated, and will inherently optimize operations as underused systems are retired. Post-migration, organizations which do not have efficient monitoring tools in their traditional data centers may gain better insight into system usage, composition and structure through Cloud Service Provider (CSP) tools.

As part of the application rationalization process, application owners should identify possible Software as a Service (SaaS) or Platform as a Service (PaaS) solutions to further limit what's carried forward. In general, IaaS should only host inherently governmental systems.

As part of portfolio consolidation, IT leaders should ensure that migrated applications do not duplicate enterprise functionality. The duplicative nature is a corollary to the commoditized solutions, but looks at the *breadth* of solutions. If twenty ticketing systems are being migrated instead of one, a stronger business case arises to consolidate on *one* SaaS ticketing solution and forego the IaaS migration of twenty separate but similar systems.

Finally, application owners want to evaluate new modernization opportunities which are not available with a traditional data center, such as serverless architectures, where organizations are charged *by the number and duration of a method call* (e.g. microservices charged per every 100 ms). Serverless architectures allow methods to be chained together based upon different triggers to create more complex applications. In addition, such systems can be honed to ensure that methods are compartmentalized enough to deliver maximum usability.

Faster Software Delivery

Reduced Application Backlogs

Bottlenecks can exist in any ecosystem or business process. In traditional IT environments, servers are a bottleneck because they limit resources based on costs, security controls, or the level of operations staffing. The advent of virtualization significantly reduced that barrier since several servers could be

allocated per machine, creation of baseline images became easier, and the staff-server ratio decreased. However, even virtualization cannot meet all the demands of a development organization, especially those organizations which have embraced Agile to more quickly deliver business applications. Software Defined Networking (SDN) provided the basis for cloud computing, which has freed development staff to obtain server support for their backlog of development projects, proof-of-concepts, pilots, and testing environments. While faster development times are a plus, organizations need to also account for any resultant increased costs. Organizations may benefit by stressing value to senior leadership, in addition to cost (e.g., spend 10% more, but get 50% more in delivery).

Stable Testing and Production Environments

In a traditional environment, top tier servers are layered at the production level, the next best servers at the test layer, and the oldest servers used for development. These incongruent environments can increase deployment risk, which may be mitigated in a cloud environment. In a cloud environment, the resources can be inverted while maintaining a high service level.

Typically, the production layer is adequately apportioned so that the mission support systems can handle degradation from load spikes, outages, and denial-of-service attacks, but if the production layer is over-allocated, mission-critical failures may result. The development layer should have enough resources to keep expensive development staff working at peak capacity. Hiccups in development environments can equate to significant aggregate hours of lost developer productivity.

What remains is typically allocated to test environments, which come in many flavors. Organizations typically have test environments for scenarios such as:

- Code being propagated to production;
- A user acceptance test (UAT) environment;
- Temporary, non-functional testing for performance, load balancing, and availability; and
- A “hot fix” environment for testing important corrections needed in the production environment.

If an organization has multiple releases being worked on by different development teams, then the number of required environments, and associated costs, can increase significantly.

The limitation of server and environmental support infrastructure can lead an IT organization to adopt a time sharing approach to test environment(s). This approach requires the configuration management team to setup and teardown environments based on the most pressing need. This setup and teardown can be costly and prone to error, because databases, server software, and applications need to be “rolled” to the correct versions for each test. Note that while creating more test environments is easier in the cloud, it can also be more expensive if the Government agency does not have good governance over their test environments.

Organizational Readiness

A cloud transformation includes more than just an acquisition vehicle. Significant organizational introspection needs to be done to ensure that the organization is well positioned for change. Below are some considerations in making an "organizational cloud transformation."

Operating Mindset Change

Own Versus Rent

Aside from the publicized OpEx versus CapEx opportunities, the buy versus rent paradigm also illustrates how organizations can become culturally attached to physical (or virtualized) server assets. In a traditional environment managed by technology professionals, servers often acquired personalities of their own, and names based upon characters and places from pop culture. As IT environments grew and became more geographically diverse, names grew more canonical to effectively inventory assets, but IT specialists still knew the servers' individual quirks and "personalities".

In a cloud based environment, servers are ephemeral and may not develop personalities as operators have become accustomed to. Just as Fonzie knew where to strike the jukebox to get it to run, so too do IT specialists know about the individual quirks their servers may exhibit.

Server Management

As IT environments evolved, many vendors invested in complex user interfaces to help system administrators manage users and server permissions. In an environment where the IT software delivery pipeline speed was set by physical bottlenecks, system administrators were capable of handling the load with the assistance of drag-and-drop functionality instead of the usage of a Command Line Interface (CLI).

In a cloud environment where servers and environments can be rapidly deployed, CLI-based scripting becomes essential to rapidly deliver services needed with minimal error in replication. In turn, scripting tools are essential to deliver cloud services.

In a traditional IT infrastructure, operations staff may be responsible for functions such as server backups and DR coop, functions which may no longer be relevant in a cloud environment. Even if there are no such services evidenced in the layout and design of the cloud environment, organizations are under the CSP SLA (e.g., Amazon[4] and Microsoft[5]) and still need to account for redundancy and uptime.

Maintaining a Skilled Workforce

System administrators and other IT staff involved in the maintenance of physical hardware may worry about lack of skills or job loss with a move to the cloud. However, IaaS still requires server and networking knowledge. Staff can acquire these premium in-demand skills (see the staffing cost section),

[4] *See:* https://aws.amazon.com/ec2/sla/
[5] *See:* https://azure.microsoft.com/en-us/support/legal/sla/

and will be released from the physical location requirements of the job. Funding for proper training may be a challenge, so organizations need to be ready to invest surge training funds to launch a cloud effort with existing staff.

Governance

As previously identified, application rationalization offers opportunities for modernization, but the IT leader needs insight into the entire IT stack. Operations, development, and security staff require tight integration and coordination to maximize efficiencies.

Application Efficiencies

Code

As hardware and memory became cheaper to *own*, code efficiency could be relaxed since there has not been as large a financial impact on the organization. In a cloud environment where services are *rented*, code efficiency regains importance as an *ongoing* (vs. one-time) savings. For instance, if an application can use serverless architectures instead of running an application on a server, the organization can employ cost models built upon microseconds, not hours, of use.

Storage

Cloud technologies provide organizations with multiple storage options with different price and usage structures (e.g., transfer charges, long-term storage). An organization needs to understand existing and future data access needs to effectively design where the data resides. As an example, the IaaS CSP solution may not be a cost effective storage mechanism for resources such as a large PDF on a website, due to high transfer charges. Usage of alternative, traditional web storage companies may be more cost effective than using the storage solution provided by the IaaS CSP.

Security Posture

Data Security

IT organizations may have concerns about data loss and cloud usage. However, current IT security best practices use techniques such as encrypted databases, random salts, public key infrastructure, and two-factor authentication to ensure that IT assets are properly secured at the data layer.

The argument of losing data control in moving to the cloud becomes relevant if the compensating controls are **the** security controls. As an example, if the data at rest is *not* encrypted, then the compensating security control is that the server resides behind physical barriers and the console is only accessible by a few properly vetted individuals. Once the *physical* compensating control is removed by migrating data to the cloud, that data would be exposed.

Identity Providers

One of the first tasks to tackle is how an agency will utilize the existing identity store in a cloud environment to effectively manage user access to cloud resources. Chances are any cloud migration will take some time, and include an already-established user directory. Multiple solutions exist which can replicate on-premise directories as well as federate with existing directories.

Migration Considerations

If an organization has developed the business drivers and is organizationally well positioned, they should also consider what gaps need to be considered between their existing IT business environment and the cloud destination.

Pricing Structures

While the CapEx versus OpEx advantages have been touted, it can be easy to overlook the specifics of different types of charges. Research into each CSP's cost models should be done to ensure an understanding of how the different services are charged for. For instance, some CSPs charge in minute increments, whereas others charge in hourly increments. Some CSP customers can get multi-year enterprise agreement discounts, and usage credits under developer programs. In some CSPs, customers can save costs by leveraging paying for server credits up-front, bidding on excess capacity, or utilizing a serverless architectures. Knowing the cost drivers is also key. For instance, if the model is built upon items such as compute power, storage space, data output, and key management and teams forget about data output, they may face a large bill after they stream a video or have many downloads of a large PDF.

Virtualization

Many traditional IT organizations have invested in on-premise virtualization and should be aware of the import (and export) features different IaaS providers offer and what formats they support. In addition, they may need to ensure staff is up-to-speed on the scripting mechanisms available, since that may be the only mechanism available. If an operating system unsupported by the CSP needs to be migrated, the server may need to be reconstituted from scratch.

Although a direct lift of the virtualized resources to a cloud environment may not achieve cost savings available via re-architecting applications, virtualization, and/or containerization of an on-premise environment can serve as a first step to migrate to a cloud environment.

The Cloud is NOT Infinite

Cloud resources are **not** infinite. For example, a CSP may offer the purchase of set aside server configurations which will be available when needed, whereas their regular on demand resources **can** run out for a particular configuration. Also, the CSP may have hard and soft limits set on resources which can or cannot be increased. Finally, different CSP environments may require CSP staff to increase soft limits, so knowledge of the lead time required is important. If any CSP limits are not effectively managed, then new servers may not be available to spin up when needed. The management of limits is akin to managing software licenses, and they should be part of a single employee's duty.

Not All Services are FedRAMP'd

Although CSPs offer numerous services, not all have FedRAMP approval. For example, AWS[6] and Azure[7] only have had a fraction of their total service offerings FedRAMP approved. Also, not all those FedRAMP-approved services are available as federal offerings (e.g., AWS GovCloud, Azure Government), or in all geographic regions. In addition, some services may be available in a federal offering but not be FedRAMP approved.

Although an agency is not limited to using just FedRAMP'd services, the organization needs to be aware of which services they'll need so that the commensurate security processes are performed for an agency authorizing official to grant an ATO for the environment to be used. Many agencies limit usage to FedRAMP approved services only.

Third Party Product Support

Support for Existing Solutions

Not all vendors have cloud equivalents for their existing products. Many IT shops have invested heavily in physical solutions for which vendors do not have an equivalent solution in the cloud, and they may need to "repurchase" the same solution in the virtual environment. If there is **not** an equivalent product, IT staff will need to find a product to meet the business need and be trained in how to use the new tool. Please note that this can also include operating systems and databases.

Functionality Gaps

The cloud partner ecosystem is still evolving, and there are numerous areas for opportunity unfulfilled by cloud service providers. CSPs provide abundant features, but no product may exist to meet a cloud management need.

Software Licensing

Licenses need to be properly allocated - some vendors will license per CPU/year, and if the environment uses a Bring Your Own License (BYOL) concept along with auto-scaling features, more instances can easily be spun up during a busy period than licenses exist. Any migration activity should ensure that licensing is included in the pre-migration planning. The licensing model should be optimized for business needs. BYOL may be effective for steady-state servers, and licenses bundled in on-demand servers for burst periods.

[6] *See:* https://aws.amazon.com/compliance/services-in-scope/
[7] *See:* https://www.microsoft.com/en-us/TrustCenter/Compliance/FedRAMP

Product Acquisition

The acquisition models used by the CSPs for third party can introduce complexities for federal usage. For example, if the CSP could have a marketplace akin to an app store where third parties can provide solutions which charge based upon **metered** usage and are charged to the CSP account. Hence, if someone has the correct rights, they can install a new solution and bypass the federal acquisition process. In addition, some regions a CSP supports may have no vendor market whatsoever, making usage a barrier for those solutions that are acquired through the federal acquisition process.

Organizational Impacts

An "organizational cloud formation" will entail numerous changes in an organization's staffing and operating procedures. This section provides an organization with considerations to assist in being "cloud smart."

Staffing

Many organizations have made a migration with the assistance of a cloud expert, but were then left to fend for themselves after the initial migration was complete. As they make such a journey, any changes can result in insecure configurations, outages, and lack of full functionality because the existing personnel were not prepared.

Existing Staff

From a technical perspective (FedRAMP aside), traditional operations staff and traditional development staff do not have the skills to maintain a cloud environment. Operations staff may have a hard time thinking of services instead of servers and storage. Although development staff may be familiar with build tools and services, they tend to lack the networking knowledge to make the environment work. In addition, the way tasks are currently done will change. For example, organizations may shift away from server specific scheduled tasks or cron jobs to use CSP microservices.

New Skills

Effective cloud management requires adding new roles to existing job duties or creating new positions. For example, in a traditional IT environment, cost containment is usually an up-front exercise (i.e., ensuring the server is acquired for the best price). However, in a cloud environment, it is an **ongoing** duty. An individual should be assigned to ensure that server sizes are not over-allocated or idly running. The management can be controlled manually, by scripting, or by using an automated tool. Each scenario requires an individual to manage the process. Another example is managing hard and soft resource limits imposed by the CSP, communicating thresholds to staff, and increasing soft limits before exhausting them.

Some CSPs may force IT staff used to a heavy graphical user interface environment to learn a CLI and a scripted language to effectively manage resources. Finally, keeping up with new service rollouts from the CSP and how it impacts the environment is a role in and of itself (for an example of the number of changes CSPs can have, *see* AWS[8] and Azure[9] updates).

Contracted Cloud Professionals

Contracted cloud professionals may not have public sector experience or be knowledgeable of federal

[8] https://aws.amazon.com/new/
[9] https://azure.microsoft.com/en-us/updates/

restrictions. Therefore, they may be adept at developing a solution, but they may develop that solution using a **commercial** toolbox of CSP services. For example, only some CSP services may be FedRAMP approved, so any solutions architected not using that subset will require additional agency resources (funding) for the C&A. In addition, an agency may be paying for an expert who has a full breadth of cloud service skills but only using a fraction of that knowledge.

Costs

Cloud IT specialists incur a hefty premium versus their traditional equivalents. Until cloud becomes the norm, IT cloud specialists can cost approximately 20-30% more than traditional IT specialists. In determining whether to train up, augment, or replace existing staff, an organization should balance not only the existing system and institutional knowledge, but also perform market research to compare federal schedule rates for cloud equivalent contract filled positions and utilize career sites to compare salaries for FTE filled positions.

Cost Controls

Operational cost control is a discipline necessitated by a cloud environment. Capacity planning should be done to ensure servers are a right fit for their use, and unused servers need to be shut off. More mature organizations will develop scripts or acquire tools to automatically shut off unused services (either orphaned or not used after hours) so that additional cost is not incurred. Several third party tools also exist to monitor and control costs in a cloud-based environment. As previously mentioned, understanding the CSP's cost model is paramount and should be revisited on a routine basis to determine whether better pricing paradigms are available or feasible. For example, if you are using resources 24x7 for an extended period of time (and will be used in the foreseeable future), then you should explore if the CSP has discounts to pay for those services up front.

Lexicon

The lexicon used for a cloud environment can differ significantly from a traditional IT environment. For example, a firewall in some CSPs is referred to as a "security group", yet a "security group" in a traditional IT environment using Active Directory refers to the common rights assigned to users in that group.

The lingua franca has significantly changed from a traditional IT environment, and ensuring that staff have an understanding of the same concepts will take time. In addition, terminology between CSPs can differ.[10]

Contracting

Cloud services are **metered** services and **should not** be contracted using Firm Fixed Price (FFP) models. Traditional contracting practices deem FFP as the most advantageous to the Federal Government, and IT leaders need to ensure that contracts are appropriately structured. Cloud services should be contracted

[10] Microsoft. "AWS to Azure services comparison." 3/17/2017. https://azure.microsoft.com/en-us/campaigns/azure-vs-aws/mapping/

out independently of cloud system integration services. Coupling the two can lead to multiple cloud accounts being created and the loss of economies of scale across multiple IT projects.

A federal agency should engage contractors at the ideation phase by maximizing market research and use a SOO if cloud deployments are new to the organization. To avoid numerous contract modifications or a work stoppage, an agency should have an application inventory and a full cloud readiness review completed prior to engagement, or have it included in the scope of the work. A federal agency can also take advantage of new categorizations for cloud service, such as the new cloud SINs on GSA Schedule 70.

Flexibility

Cloud services enable IT organizations to quickly spin up proof-of-concepts, prototypes, and new environments. With that speed, organizations need to manage customer expectations, particularly around the entire product development lifecycle.

Streamlined patch maintenance and testing rapidly improves the security posture of IT systems. Entire environments can be temporarily reconstituted and tested with the latest patches. If the patches are successful, the test environment can quickly replace the production environment.

Security Risks

Security Boundaries

Using both virtualized assets and services requires a different mindset to deploy and operate cloud resources. For instance, some CSPs use tagging to delineate services and virtualized entities are controlled by logical boundaries. Even in this paradigm, the virtualized entities are usually launched into logical boundaries, but further access is controlled by tags. Management tools to more effectively handle services need to be built or acquired. Inherent in the delineation between assets and services is the security risk of IT staff incorrectly tagging or placing resources.

Segregation of Duties

Cloud IT roles do not map 1-to-1 with traditional IT roles. As a consequence, many IT professionals receive elevated privileges, which directly contrasts to following a “least privilege” paradigm. In addition, key roles can exist which are considered “high blast radius” if a user is granted them. While IT organizations are migrating to the cloud, they may grant privileges to get the job done in lieu of learning what the least privileged settings are. The risk to the cloud environment is akin to the risk application servers have faced in the past when they were granted the equivalent of root-level privileges on traditional two tier systems.

In addition, many organizations are doing more with less, so if individual users need to perform multiple tasks crossing logical Segregation of Duties (SoD) boundaries because of limited staff, they should be issued multiple roles and not using a single role with all the access needed. The organization should ensure that proper governance policies are established for accommodating users who have roles which

present a conflict of interest.

DevOps Doesn't Include Security

The usage of the term "DevOps" presents the idea that application development staff can do it all, and does not account for the need for security, or the need for an understanding of basic computer networking. DevOps is really a new role and should not be confused with the idea that existing developers can perform all operations.

Basic Encryption and Key Management

Some people may have fears that the cloud is not as secure as a traditional data center. Cloud vendors offer security tools, however, the security risk is that staff do not properly implement those security controls, either through a lack of knowledge, or by using other, outdated tools. As previously mentioned, the highest security risks involve unsecured keys or unencrypted data. To minimize access risks, organizations should safeguard any master accounts used to provision the environments (i.e., never use them except to set up the initial administrators and very securely lock away the access), choose to encrypt virtual drives, and use a key management service external to the CSP environment.

Image Management

Cloud providers may offer image management services. A good practice is to know the scope of saved images and ensure that they're not incorrectly shared. For instance, in some CSPs, machine images can be stored in a private or public repository. If a machine image is shared publically, then anyone with an account for that CSP can run that image. Organizations need to keep abreast of their CSP image management features to ensure permission scoping is appropriate for their business needs.

Audit Trails

The elasticity of IaaS poses challenges in regards to auditing services which can be very ephemeral. Organizations should ensure that they have an architecture in place which will be able to capture services which are started and destroyed within a small time window.

Policy Considerations in the Cloud

Foreign Nationals

One agency may ascribe to stricter rules in regards to CSP staff support. For example, some CSP regions follows ITAR and guarantees only "U.S. persons" will be involved in the maintenance of support. GovCloud costs more for services, and helpdesk turn-around takes about 48 instead of 24 hours since it needs to be routed to a group of U.S. persons.

Network Topography

Federal agencies may need to consider IP address allocation to adequately monitor threats via

automated tools. If an agency extends their presence to the cloud, they may need to allocate internal IP address ranges for cloud usage. However, doing so will require up-front allocations to accommodate different functionality (e.g. development, testing, production), which will limit network elasticity which could be later needed.

TIC Compliance

Trusted Internet Connections (TIC)[11] regulations are currently still in effect for IaaS usage, but DHS is working on solutions in conjunction with CSPs akin to the Managed Trusted Internet Protocol Service (MTIPS) program.[12] Agencies have implemented solutions to ensure TIC compliance such as using direct connection capabilities for CSP traffic. However, such services can be costly and represent a barrier to cloud adoption.

IPv6 Compliance

The Federal Government is required to adhere to IPv6 compliance.[13] Agencies should be aware of the IaaS cloud services which are available to meet IPv6. While some vendors may have some services which are IPv6 compliant, those services may not be FedRAMP approved.

Software Licensing

The Category Management Policy 16-1 memo includes software licensing in a cloud environment.[14] The memo indicates "OMB will encourage or direct use of best-in-class existing software licensing agreements", but the ultimate responsibility lies with the Agency Software Manager. The agency software license management policy should be adhered to when using a BYOL or bundled license model on an IaaS virtual machine.

DNSSEC

Per OMB Memorandum M-08-23: "Securing the Federal Government's Domain Name System Infrastructure",[15] agencies need to ensure they implement DNS security "to all Federal information systems." The requirement would also extend to any IaaS service using DNS.

HTTPS-only

As stated in OMB Memorandum M-15-13,[16] "all publicly accessible Federal websites and web services only provide service through a secure connection." While DNSSEC ensures endpoint security, HTTPS-only

[11] Department of Homeland Security. "Trusted Internet Connections." 3/16/2017. https://www.dhs.gov/trusted-internet-connections
[12] General Services Administration. "Managed Trusted Internet Protocol Service (MTIPS)". 3/13/2017. http://www.gsa.gov/mtips
[13] National Institute of Standards and Technology. "Special Publication 800-119: Guidelines for the Secure Deployment of IPv6." 12/2010. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-119.pdf
[14] M-16-12. Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing. 6/2/2016. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf
[15] M-08-23. Securing the Federal Government's Domain Name System Infrastructure. 8/22/2008. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf
[16] M-15-13. "Policy to Require Secure Connections across Federal Websites and Web Services." 6/8/2015. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf

ensures data is not intercepted or manipulated in transit.

Chargebacks

Implementing a chargeback mechanism can recoup base IaaS charges along with federal value added services such as agency implementation of FISMA controls. The reselling of IaaS services via chargeback mechanisms can result in consuming components losing an hourly measured rate option and being forced to pay for services using a longer duration (e.g. a month). Such a cost model significantly erodes the benefits of a "pay as you go" scheme.

Funding

In a traditional CapEx model, servers can be acquired using year end funding. That alternative is not available using IaaS services, and continuity of operations needs to be ensured across fiscal years. The issue can be further complicated by federal shutdowns. Even if servers can be shut off so that the metered fees are not incurred, costs associated with the storage of those images are still incurred. In an IaaS model, an effective plan needs to be in place to ensure funding lapses do not affect work.

Section 508 Compliance

Contracts with CSPs need to account for Section 508 compliance (e.g. so that all staff can use web interfaces or toolkits to interact with CSPs).[17] While contract clauses may cover 508 compliance at the time of procurement, the contract requirements need to take into account the nature of service offerings in the cloud to denote that any new services made available are also 508 compliant.

For additional information regarding this paper or topic, please contact the DCOI Managing Partner program management office at dcoi@gsa.gov.

[17] Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794 (d)). *See:* https://section508.gov/content/learn/laws-and-policies