MANAGING MULTIPLE CLOUD IMPLEMENTATIONS
BREAKING DOWN WHAT YOU NEED TO KNOW

GOVLOOP POCKET GUIDE 2017
AGENCIES MUST BALANCE THE NEED TO HAVE THE RIGHT CLOUD FOR THE RIGHT USE CASE WHILE ALSO ENSURING THEY CAN PROPERLY MANAGE THOSE CLOUDS
Then add to the confusion different applications with different requirements for performance, service levels and latency. These needs won’t disappear once you move to the cloud. So how do you meet all of those demands in an efficient and economical way?

Today many organizations are moving to a "multi-cloud" strategy, where they employ multiple cloud architectures at the same time to get the optimal performance for the best value. In this case, several independent cloud architectures are implemented, and each supports its own set of applications and users. Although the term may be unfamiliar, many government agencies have successfully implemented multi-cloud solutions and are reaping the benefits.

When choosing a cloud model, agencies have a wide variety of legitimate concerns, and there are many competing considerations that must be addressed, including:

- Security
- Compliance
- Performance
- Response times
- Availability

Organizations must define these requirements, find a system to fit those needs and implement it successfully. That process often requires the help of industry experts who understand the challenges of the terrain. Multi-cloud doesn’t have to be complicated. With the right guidance and planning, it can help your agency tackle workload hurdles.

In this pocket guide, we provide a clear explanation of everything you need to know about multi-cloud solutions and how this approach can benefit your organization — from basic definitions to real-world applications and the economic and operational reasons behind this shift in IT delivery.

We’ll explore the key steps in moving toward a multi-cloud solution and how to mitigate risk during a multi-cloud implementation. Furthermore, you’ll learn how to make a sound operational and business case and use this strategy for your agency.

We’ve packed scores of valuable information and takeaways into just a few pages for your convenience. Learn from the experts at ViON, who have been delivering on- and off-premise ITaaS and cloud for over 16 years and matching each agency’s needs with the right cloud architectures to achieve its mission. We explain why — and how — cloud is changing the way IT is accessed and delivered across the government. We also highlight how the flexibility of an as-a-Service model can offer agencies access to hybrid for multi-cloud environments with a low cost of entry. Whether you are choosing multi-cloud or any infrastructure, analytics or cloud solution, ViON is the partner your agency can trust to modernize your IT. Read on to learn more.

“Although the term may be unfamiliar, many government agencies have successfully implemented multi-cloud solutions and are reaping the benefits.”

—Ray McCay, Vice President of Solution Sales at ViON
Finding the right cloud model can be overwhelming. ViON®’s more than 16-year history of delivering on- and off-premise ITaaS and Cloud will ensure you have the right balance of value and performance. Our flexible as-a-Service model delivers hybrid solutions for multi-cloud environments with a low cost of entry.

- Overcome business barriers to the Cloud
- Minimize financial risks with the right financial model
- Simplify cloud management and infrastructure migration
- Meet complex security requirements

Learn more about how we can remove barriers to the Cloud and contact us directly today.
With any change in administration comes new priorities and initiatives. Sometimes those initiatives are a complete overhaul of what took place under the previous administration. Other times the focus is on enhancing the work that’s already in place. For the federal government, investments in cloud computing fall into the latter category.

In May 2017, President Donald Trump issued a cybersecurity executive order that, among other things, requires agencies to “show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.”

For years, cloud computing and cybersecurity have been at odds because agencies questioned whether cloud service providers could adequately protect government data. But thanks to programs like the Federal Risk and Authorization Management Program (FedRAMP), which standardized cloud security, agencies are now embracing cloud as a secure option for hosting even mission-critical systems.

In May 2017, President Donald Trump issued a cybersecurity executive order that, among other things, requires agencies to “show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.”

For the federal government, investments in cloud computing fall into the latter category.

For years, cloud computing and cybersecurity have been at odds because agencies questioned whether cloud service providers could adequately protect government data. But thanks to programs like the Federal Risk and Authorization Management Program (FedRAMP), which standardized cloud security, agencies are now embracing cloud as a secure option for hosting even mission-critical systems.

The executive order calls on the White House director of strategic initiatives to coordinate with various agency heads to develop a report detailing the legal, budgetary and technical feasibility of moving all agencies — or a subset of them — to a consolidated network architecture and shared email, cloud and cybersecurity services.

Cloud adoption is sure to receive ongoing attention as both congressional lawmakers and the White House work to move agencies off legacy technology to more modern IT. “Modernization, in this sense, is not simply replacing individual outdated IT systems with newer ones; rather, it is a holistic approach to federal IT that fundamentally transforms how agencies accomplish their missions,” according to the president’s fiscal 2018 budget proposal.

The proposal acknowledges that agencies will need to reengineer underlying business processes and adopt modern IT solutions, such as cloud and shared services.

Office of Management and Budget policies already encourage the use of provisioned services, such as cloud, and that is expected to continue. According to the CIO Council’s State of Federal IT report issued in January 2017, agencies expected to spend more than $2 billion on cloud computing services out of a total of $80 billion in IT spending in fiscal 2016.

But, with any new business model comes challenges. The urgency to move to cloud resulted in rushed planning cycles and decisions. Early thinking that one cloud deployment could do all that was required has given way to a multi-cloud scenario. Agencies are now beginning to wrestle with the more complicated, but required, challenge of managing multiple clouds. They must balance the need to have the right cloud for the right use case while also ensuring they can properly manage those clouds. In many situations, agencies look for help from cloud service providers.

This new pocket guide will give you an overview of the current landscape of multiple clouds in government, explain how we got here and why it’s so crucial, as well as provide a brief overview of the difference between hybrid and multiple clouds. The guide also includes case studies and common challenges and solutions for managing a diverse cloud environment.
 Agencies are using a variety of different cloud environments to meet their needs. In this section, we define multiple cloud implementations, what’s driving it and some of the challenges that agencies face.

In the world of government IT, applications are not created equally. Depending on the application, requirements for success will vary. Considerations include performance, availability, service response times, business continuity, backup and recovery, security, compliance, data custody, and many more.

All of these factors must be considered as agencies choose the right types of cloud to support their applications and meet their computing needs. They need to bring together the right cloud infrastructures and cloud business models that can satisfy their individual application requirements.

The nuances of each application and dataset caused agencies to design different cloud architectures or business models to accommodate these variations. The result for some agencies was the creation of different clouds — in silos. The challenge now is managing this ecosystem of multiple architectures, technologies and cloud service providers.

“Overall cloud computing growth this year has led to an increased proliferation of a multi-cloud type environments, including hybrid,” according to the General Services Administration’s 2017 Hybrid Cloud Almanac. The report’s statistics, which are based on a survey of more than 1,000 IT enterprise technical professionals, show that on average, cloud users are leveraging six clouds. In addition:

- Seventeen percent of enterprises now have more than 1,000 virtual machines in public clouds, up from 13 percent.
- Private cloud use has increased by 22 percent among enterprises.
- Hybrid cloud adoption has increased by 13 percent year to year, while overall cloud adoption has increased 2 percent.

It’s becoming more common for agencies to mix and match multiple cloud providers and solutions in pursuit of the best fit for their agencies’ needs. Although managing this diverse environment isn’t without challenges, agencies want to reap the benefits of having options.
For example, an agency might use Azure’s public cloud offering to host citizen-facing websites but opt for other vendors and solutions to manage email services and more sensitive data in a private cloud. Agencies may choose yet another vendor for a hybrid cloud deployment. Also, high security environments and associated requirements will often drive the selection of a separate cloud environment. There are just a few public cloud providers, Azure being one, that can meet these stringent security standards set by the defense and intelligence communities.

The key is having a strategy for adopting and managing various clouds deployments, each designed appropriately to meet the requirements of the application environments they serve.

In its 2017 State of the Cloud Report, Software-as-a-Service firm RightScale found that more enterprises have a strategy to use multiple clouds. Of the more 1,000 technical professionals surveyed, 85 percent said they have a strategy, compared with 82 percent in 2016. There was also an increase in the number of enterprises planning for multiple public clouds but a decrease in those planning for multiple private clouds.

For early adopters in government, cloud strategies didn’t tend to focus on managing multiple clouds. Instead, they centered on simply getting to the cloud — any cloud — and reaping promised cost savings and efficiencies. But agencies soon realized that their security, data and procurement requirements should drive their decision-making.

For example, many agencies with data custody concerns opted to manage data in a private cloud. When they needed disaster recovery capabilities, they considered a public cloud. But they also wanted help managing the environment and monitoring the usage of those clouds, so they implemented a hybrid cloud environment.

There are also situations where agencies are concerned that a public cloud provider might go out of business or suffer from service outages, so they diversify their offerings and put their data in two clouds. Another concern is the risk of vendor lock-in, which impedes agencies’ ability to move their data from one cloud vendor to another. To reduce this risk, agencies should include in their contracts explicit service level agreements for security, continuity of operations and service quality that meet their individual needs. Having an exit strategy that details how data will be moved securely and efficiently from a cloud environment is also crucial.

Your agency may be dealing with competing interests and trying to manage multiple clouds. That’s why these precautionary steps are critical to ensure operations at your agency aren’t hindered, especially if you move to another cloud provider. If your current cloud ecosystem looks at little like the Wild West, getting a handle on managing that environment must be a priority.

### TIPS FOR MANAGING MULTIPLE CLOUDS

1. **Use Cloud Models that Provide an Interoperable and Portable Environment**
   - for data and systems. This will make it easier to move workloads between common services and platforms.

2. **Craft Service-Level Agreements and Contract Language that Provides a Clear Exit Strategy for Leaving a Cloud or Shifting Between Environments.**

3. **Map Out a Business Continuity Plan**
   - in the event that services are disrupted in any of your clouds.

4. **Scrutinize Your Backup Strategy,**
   - including data sensitivity, compliance, and security.

5. **Automate Processes**
   - to manage multiple cloud environments remotely as much as possible.

6. **Invest in Multiple Cloud Architectures,**
   - consider security, compliance, performance, service response times, application profiles and connections, availability and mission criticality of applications. Make sure that each is properly positioned in your SLAs.

7. **Ensure Your Cloud Partner**
   - can work with you every step of the way, including planning through implementation across clouds for various workloads and use cases.
HYBRID CLOUD VS. MULTIPLE CLOUDS

You may hear hybrid and multi-cloud used interchangeably, but they aren’t the same thing. In this brief section we explain the difference between the two.

HYBRID CLOUDS

Hybrid cloud is the creation of a cloud architecture that uses more than one underlying approach. For example, a hybrid cloud might be one that joins a public cloud implementation to a private, on-premise implementation and perhaps adds managed services. Those third-party services can augment your in-house capabilities and include managing the performance of storage infrastructure, networks and applications.

MULTIPLE CLOUDS

Multiple clouds or multi-cloud means you have deployed multiple different clouds at the same time. For example, several independent cloud architectures have been implemented and each supports its own set of applications and users. Perhaps one is an all-public cloud implementation, and another is a hybrid model connecting private and public clouds together. You may have another architecture that’s a firewall-protected private cloud.

RELEVANT STATISTICS

ADDRESSABLE CLOUD COMPUTING BY BUYER SEGMENT, FY 2016-2021 ($M)

Source: Deltek
Cloud adoption in government is on the rise, thanks to key administration efforts focused on reducing federal data centers and moving to secure cloud environments. That ongoing journey hasn’t been without challenges, but agencies are gradually reaping the cost savings and efficiency benefits of cloud. Here are a few of the initiatives that have had the greatest impact on government cloud adoption:

**June 2012**

The Federal Risk and Authorization Management Program launched operations. The governmentwide program integrates standards and risk management with Cloud First. It gives agencies a standard way to continuously assess the security of cloud products and services.

**December 2014**

The Federal Information Technology Acquisition Reform Act (FITARA) becomes law. It requires agencies to submit annual reports that include data center inventories, strategies to consolidate and cost savings — among other things.

**August 2016**

The Data Center Optimization Initiative updates FDCCI, based on requirements set by FITARA. It shifts the focus to optimization metrics, in addition to cost savings and closures.

**May 2017**

A new cybersecurity executive order requires agencies to “show preference in their procurement for shared IT services, to the extent permitted by law, including email, cloud, and cybersecurity services.”
THE JOURNEY TO CLOUD STARTS WITH THE RIGHT QUESTION

Depending on whom you ask, you'll likely hear different reasons for why agencies are migrating to cloud. The reality is agencies have varying needs, and while one may be interested solely in cost savings, another may see cloud as a way to free up staff for other projects.

Whatever the reason, it's critical that agencies clearly define why they are moving to cloud before they take the leap. That's the first question ViON's Ray McCay asks before teaming with customers on cloud investments.

"You would be surprised at how many times what you get back is dead silence because somebody has been told the cloud is a good thing, or that they're archaic if they are not in the cloud," McCay said. "Well, cloud is a good thing, but the journey starts by asking what are you trying to do with cloud?"

Thinking through the problem you want to solve will save you time, money and unnecessary headaches in the long run. McCay offered several best practices to consider in the event that you're already maintaining the leap. That's the first question ViON's Ray McCay asks before teaming with customers on cloud investments.

"Driving cost efficiency and achieving mission success while supporting sizeable application inventories and associated diverse requirements, will typically result in a multi-cloud deployment."

—Ray McCay, Vice President of Solution Sales at ViON

In some instances, people automatically assume moving to the cloud means a public cloud. But that is not an assumption that agencies should make. McCay warned against getting hung up on the type of cloud and recommends that agencies focus instead on their needs. From there, a well understood success plan will dictate the type of cloud architecture that serves best, whether public, private, hybrid or multi-cloud.

"That's where it starts — a well understood success plan that defines application requirements and spells out what is needed for mission success," he said. "Multiple clouds will likely result because application requirements vary greatly. Driving cost efficiency and achieving mission success while supporting sizeable application inventories and associated diverse requirements, will typically result in a multi-cloud deployment."

The most desirable end state for agencies with multiple clouds is one where they can use a single interface to manage all their cloud deployments. The technology exists to do it. ViON has an interface that customers can use. But the challenge is that people operate independently, which makes it hard to manage technology in a unified, consolidated manner.

It comes down to policy. The agency has to ensure that people are following protocols and not swiping a credit card to buy IT infrastructure without any parameters.

Once you've defined your goals for cloud and completed an application profile, you're ready for the design phase, ensuring your targeted cloud design is fully capable of delivering what you need. Next comes the build and deploy phase, then finally the migration plan. This roadmap should define the steps you'll take to move from your current environment to the cloud. "Don't try to go too fast and jeopardize the success of the project," McCay said.

ViON offers Professional and Managed services to help agencies move quickly to a cloud business model leveraging modernized IT technologies with best in class performance and availability, without first having to complete the full cloud transition roadmap or even their application profile. ViON will deploy a fully modernized IT infrastructure in a private cloud business model and work with the agency to complete application migration. This will allow the agency to realize substantial and immediate benefits from moving to cloud. Then application profiling and further transformation planning can be conducted in a more leisurely and less risky fashion.

It enables agencies to greatly accelerate the value derived from a cloud business model. The overall goal is to reduce the time it takes to realize the value of cloud, whether that’s improving the performance of an application or moving from Capex to Opex spending. With ViON’s offerings, agencies can begin reaping those benefits in a matter of weeks versus years.

Agencies can decide whether they want to manage their cloud environments with their own people and resources or partner with ViON to take on those tasks for them — in part or in whole. "ViON is flexible, we are here to assist as an agency has need. We can do as little or as much cloud management as agency desires," McCay said.

As cloud adoption matures across government, agencies must also evolve their cloud strategy. Early on, the focus was simply getting data and workloads to the cloud. But agencies must also think strategically about how cloud deployments will drive mission success.

"That's really our motto, to achieve mission success for our customers," McCay said. “Our goal is to make sure that our customers achieve the business objectives they had in mind.”
LEARNING FROM OTHERS: CASE STUDIES

Now that we’ve explored the basics of maintaining multiple clouds, here are a few examples of how agencies have overcome their computing challenges while lowering costs and boosting efficiencies.

DEFENSE AGENCY

Complex procurement processes, lengthy acquisition timelines, and rapidly changing storage requirements are common challenges for any government agency. But at one defense agency, in particular, these challenges made it hard to support the management and storage of sensitive data for its customers. Hardware was often warehoused awaiting deployment, which was costly. The agency was looking for a more effective way to balance storage requirements without paying for unused technology but providing rapid scalability.

That’s where ViON came in. The company provided an easy-to-use call order portal, which simplified procurements by providing a streamlined ordering process. It also provided the agency visibility and ensured better control of project schedules and budgets. Responsiveness was also key. ViON facilitated the agency’s ability to meet urgent provisioning needs when critical workload changes were required.

Teaming with the defense agency, ViON used an agile acquisition model to provide enterprise data storage assets at multiple sites within the U.S. and overseas. This flexible model used operational expenditure funds and enabled the agency to scale resources up and down without fees or penalties. That way the agency paid only for what it used and provisioned additional storage on an as-needed basis.

This reduced the agency’s storage infrastructure costs to meet the demands of data center consolidation and transformation efforts.
This federal healthcare agency was challenged to provide secure, highly available, enterprise disk storage to meet the needs of its client agencies.

Its IT Department was managing multiple data centers with outdated legacy infrastructure and budgets were overrun with excessive maintenance costs. In addition, it lacked resources to provide acceptable response time for issue resolutions.

ViON provided a flexible, highly reliable and cost-effective storage Infrastructure-as-a-Service that enabled the agency to scale capacity up or down, as needed. ViON worked with the agency to plan for migration and deployment of new storage technology to replace outdated systems, reduce downtime, and eliminate excessive maintenance cost throughout the contract.

ViON also closely monitored and proactively managed the infrastructure for the agency to improve response times and reduce error rates. This ensured the highest level of availability and efficiency for the agency’s evolving workloads.

A lengthy acquisition process was among the many challenges plaguing this federal civilian agency. Add to that list overprovisioning of storage and vendor lock-in issues, which caused unnecessary and costly outages, downtime and inadvertent cross-charging across departments.

In addition, the agency lacked the capability to show internal customers’ storage utilization control, and it suffered from poor storage utilization and management. This resulted in costly underutilization of storage.

To address these issues, ViON provided the up-front investment in equipment and technology, mitigating the financial risk to the agency. ViON’s flexible model scaled up and down without fees or penalties on an as-needed basis without service interruption. In this full managed service environment, ViON personnel were directly responsible for the provisioning, management and reporting infrastructure.

ViON also provided a secure, web-based management portal to simplify the procurement process. With this streamlined process came greater visibility and better control of project schedules and budgets.
WHERE DO I START WITH CLOUD?

1. Define business objectives for moving to a cloud model.
2. Look at your end user communities and their service level expectations.
3. Examine your applications, and determine their individual requirements.
4. Identify your compliance requirements and security and data custody needs.

5. Develop an overall application profile services engagement to gain visibility to your application dependency.
6. Gain quick benefits by first moving your applications to an on-premise or off-premise, modernized private cloud model.
7. Then take a more leisurely approach to moving your applications to the appropriate cloud business deployment model.

How to Embrace Cloud as a Business Model

IT-as-a-Service 101: Breaking Down What You Need to Know

Mapping Your Path to the Cloud
PARTNER WITH ViON TO ENSURE YOUR MULTI-CLOUD PROGRAM IS OPTIMIZED.

About ViON
Designing and implementing innovative solutions that meet dramatically changing IT requirements is ViON’s mission. Founded in 1980, we’ve grown from a small product reseller into a leading systems integrator delivering customized solutions and best of breed offerings from the world’s premier OEMs to large public and private organizations. Known for our engineering expertise and exacting standards, ViON ensures that only those with the highest level of training, experience and industry certifications design, install, maintain and support our breadth of solutions. We focus on data management, so you can focus on your organization’s success. We’re on the leading edge of Advanced Analytics, Cloud and Data Management. ViON’s cloud-based “as a Service” Program Management Office delivers direct access to the technology you need for today and tomorrow. From the data center to the cloud, let ViON’s passion for innovative solutions secure the competitive advantage required for your enterprise. Learn more at www.ViON.com.

About GovLoop
GovLoop’s mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com
As cloud continues to transform the way services are delivered across government, agencies are embracing multiple clouds to meet their evolving mission needs.