KNOWLEDGE TRANSFER:

Becoming an Informed Cloud Buyer

DLT SOLUTIONS®

AN INDUSTRY PERSPECTIVE

INTRODUCTION

Conversations about cloud computing are a lot different today than they were four years ago. Back then, definitions for this new business model varied, and some people questioned if cloud solutions could ever be as secure as the government's internal hosting environments.

Additionally, agencies were coming to grips with the implications of information technology-as-a-service at a time when there weren't widespread government case studies on how cloud impacted internal operations, workforce and budgets.

To clear up the initial confusion around cloud, the National Institute of Standards and Technology published its 16th — and final — **definition of cloud computing** in 2011. That same year, then-federal Chief Information Officer Vivek Kundra issued the **Federal Cloud Computing Strategy**, prompting the government's shift from acquiring more assets to buying IT services. Prior to the strategy's release, agencies were instructed to adopt a **Cloud First policy** and move three services to a cloud environment by June 2012.

At the time, many would have balked at the Pentagon's recent decision to seek a commercial solution for the Defense Department's next-generation enterprise e-mail system and Hawaii's decision to move its critical human resource system to a cloud environment.

But agencies have come a long way since the pioneering days of cloud computing.

Today's government consumers are more educated and have at least tested the waters when it comes to moving data and applications to external providers. Agencies are taking advantage of the Federal Risk and Authorization Management Program's "do once, use many times" approach to cloud security.

"Agencies have reported a total of 81 systems as being FedRAMP compliant," according to the 2**014 Federal Information Security Management Act report to Congress**. A total of 26 agencies have reported using FedRAMP provisional authority to operate packages, and that number is growing. These documentation packages verify that cloud solutions meet federal security standards and help streamline the process of greenlighting solutions for agency use. Many credit FedRAMP standards with accelerating government cloud spending. Although the number of cloud investments has increased, spending has not yet reached the projected $20 billion that agencies **estimated could move to the cloud**.

The **president's 2016 budget proposal** notes that cloud computing and other provisioned services account for about 8.5 percent of federal IT spending today. As cloud spending increases and the market grows, agencies want to ensure they have solid contracting language in place and the right support to implement and manage the full life cycle of cloud deployments.

GovLoop and DLT Solutions, an IT solutions company that provides public-sector customers with a simplified path to the cloud, are here to help. David Blankenhorn, Vice President of Engineering and Chief Cloud Technologist at DLT Solutions, recently spoke with GovLoop to clear up lingering misconceptions about cloud technologies and offer best practices for identifying cloud-ready applications.

Whether you're a cloud novice or further along in your cloud journey, this report will help guide you through the changing IT landscape.

CLOUD COMPUTING MYTHS YOU SHOULD STOP BELIEVING

There's no doubt that cloud consumers are more informed than they were a few years ago. They understand the basics of cloud, what it is, what characteristics to look for and the various as-a-service deployment models. But despite this heightened level of awareness, misconceptions still abound, and it's time to clear them up.

Roles & Responsibilities

Moving to the cloud doesn't mean that agencies relinquish complete control and responsibility of their data. Cloud is a team sport, and this is particularly true in the area of security. The reality is every cloud service provider (CSP), regardless of the platform, has a shared responsibility to keep agency data secure. For infrastructure and platform offerings, agencies must address several security controls.

Infrastructure-as-a-Service consumers generally take on greater responsibilities for implementing security controls because they must assume the roles of integrator and operator. That doesn't mean infrastructure providers are off the hook for implementing security and privacy safeguards. Instead, they are responsible for "providing protections at infrastructure levels that a consumer does not have control of," **according to NIST**.

"The best rule of thumb is that [when dealing with Infrastructure as a Service] the CSP is responsible for everything from the abstraction layer all of the way down through the physical infrastructure," Blankenhorn said. "The customers are ultimately responsible for managing everything that they put within that cloud — be it code, applications, identities, data and the daily operations of the elements that the customer puts in that CSP."

Virtualization vs. Cloud Computing

The terms virtualization and cloud computing are commonly used in the same breath, but they aren't synonymous. Cloud computing is not an outsourced version of the virtualized server environment in your data center, Blankenhorn explained. Cloud requires a completely different architecture and delivers different value. The implementation and management demands are also different from virtualization.

"Virtualization is very good at resource pooling, and it has broad network access at least within the customer's environment (which isn't a bad thing)," Blankenhorn said. "However, virtualization often fails to support the on-demand, self-service and measured service (i.e., granular chargeback, based on actual utilization of the resources), and it struggles with the 'rapid' component of rapid elasticity, as IT is often the team for provisioning the resources, whereas in a cloud platform the provisioning is fully automated."

Similar to cloud computing, **virtualization technologies** can help agencies operate their information systems more efficiently and reduce hardware, energy and maintenance costs, but the end results aren't exactly the same. Think of cloud as taking virtualization to the next level in terms of self-service and rapid elasticity capabilities, both of which are key characteristics of cloud.

The reality is every cloud service provider, regardless of the platform, has a shared responsibility to keep agency data secure.

BRINGING CLARITY TO THE CLOUD

The early days of cloud computing in government were marked by a lot of hype and buzz, but also a lot of confusion, Blankenhorn said. "The vendors certainly didn't help much, and there [was] a lot of political cloud washing going on."

If you're not familiar with that term, you've most likely experienced cloud washing in some form. "Cloud washing typically refers to vendors' and service providers' exaggerated marketing, where they label a product as cloud even when such designation is either completely false or at best, jumping the gun on a future capability," a 2014 Forbes article notes.

It's no wonder that so many in government and industry struggled with how to define cloud computing. But about two years ago, conversations around cloud changed and matured as people gained a better understanding of cloud and its varying deployment models, Blankenhorn said. Today, most questions are about security.

Although programs such as FedRAMP are now in place, cloud security is a concern that will always be top of mind for government officials. The main questions Blankenhorn fields from customers focus on how they use cloud technologies securely and how they enable mission owners to securely act on their requirements with the right security paradigm and controls in place.

With technology comes risk, especially when humans are involved. Deciding what an acceptable level of risk is and how to mitigate it in a cloud environment are among the factors that must be considered.

Read the Fine Print

Agencies are particularly interested in honing their approach to procuring cloud solutions. Contracting officials want to know the appropriate method for buying services and how to choose or develop the right contract, with the right terms, to appropriately acquire cloud in the public sector.

"A lot of the [contracting officers] that are involved have tremendous expertise in the acquisition of products, not necessarily the acquisition of these sorts of on- demand services," Blankenhorn said.

When contracting cloud services, Blankenhorn suggests that buyers use traditional, product-oriented vehicles, such as General Services Administration (GSA) IT Schedule 70, the National Institutes of Health IT Acquisition and Assessment Center's (NITAAC) CIO-CS, Solutions for Enterprise-Wide Procurement (SEWP) V, or an indefinite-delivery, indefinite-quantity (IDIQ) contract. "The goal is to treat the contract as more of a time–and-materials with a 'not to exceed' style of contract rather than a firm fixed-price contract, even though you are not purchasing professional services."

Agencies must also make plans for migrating from a cloud environment in the event that a contractor is unable to operate the system. They have to consider what procedures are in place to ensure that a different contractor can successfully operate the system.

An **August 2014 report** by the Labor Department's inspector general notes that the department's transition plan should include steps for:

- Transferring system operations and special knowledge to the new operator
- Negotiating the current contractor's participation during the transition, including commitment of the current contractor's key personnel
- Transferring hardware from the current contractor to the new operator
- Defining critical processes performed by the current contractor on behalf of the department (e.g., backups, access provision, patch management and promoting changes to production)
- Transitioning problem management processes (e.g., help desk)
- Defining internal roles and responsibilities during the transition

State and local government officials are wrestling with the same contracting challenges. One in particular is deciding the appropriate amount and type of damages agencies can recoup from vendors if a data breach occurs, **StateTech reported** during a National Association of State CIOs' conference in 2014.

"In Pennsylvania, [limitation of liability is] traditionally two times the cost of the contract," said Tony Encinias, Pennsylvania's Deputy Secretary for IT and CIO at the time. "When you're talking about a $1 billion contract, there is no company in the world that can sign up for that risk. So, you have to really give and take."

NAVIGATING THE CLOUD

The risk-averse nature of government may lead some to assume that agencies are playing it safe and mainly focused on moving public websites and development and testing environments to the cloud — "you know, the usual kind of low-hanging fruit that you might think of," Blankenhorn said.

He admitted even he is not immune to this misperception. "The irony, as I ran some analytics on our own customer base, [was] dev test and public websites were actually the smallest use cases in the workloads we're seeing on, for example, Amazon Web Services," he said. "We're actually seeing much more interesting workloads on those platforms going into production."

These include geographic information systems, sharing and document management tools, and analytics applications. That's not all. Traditional enterprise workloads, such as SAP and Oracle applications, are also moving to the cloud.

"I would say more mission-oriented applications and services are absolutely being moved out there," Blankenhorn said.

With more than 100 successful public-sector cloud implementations under its belt, DLT Solutions has a pulse on the common pain points and questions that arise as well as the benefits of cloud that customers can expect. The company shares much of that knowledge with its customers through a resource called **DLT Cloud Navigator**.

DLT Cloud Navigator is a knowledge base that customers can use regardless of where they are in the cloud life cycle, Blankenhorn explained. It's the brand under which DLT addresses the full life cycle of consulting services and other offerings, including training, installation and configuration services, and daily, round-the-clock technical support from U.S. citizens on U.S. soil. Navigator was born of conversations the company had with its federal, state and local, and higher education customers after realizing they had similar questions and concerns.

The **Navigator site** offers potential use cases, technologies, and sample architectures and designs that explore what agencies can do with cloud technologies. It's really about knowledge sharing and educating consumers.

"And it's really à la carte," Blankenhorn said of the company's offerings. Customers may only want information on existing cloud capabilities in the market, he added. "We're not going to force on them the implementation or the managed services."

IS YOUR APPLICATION CLOUD READY?

There are key questions to ask and considerations to make before moving an application to the cloud. Here are a few of them:

- Who are the end users?
- Will users access the application remotely from their mobile devices or from a personal computer?
- Is it an internal application that will be accessible only to those within the agency or is it part of constituent services?
- What types of dependencies are present? Is the app connected to other applications or databases?
- How might moving that application to a public or private cloud affect performance, and will networking and latency issues have an impact?
- Do you understand your network topology and what limitations exist?
- What compliance standards or federal laws govern the protection/storage of the data?
- Do the cloud providers that are available accommodate your compliance requirements?
- Are there any physical hardware dependencies that may be involved or required by the application?

If agencies don't consider these questions, they may end up with poorly performing applications, dissatisfied end users or unexpected network upgrade costs to handle the applications in a cloud environment, Blankenhorn said. Customers should also consider how a provider operates its cloud environment and whether it has the right skills to support them and deliver quality service.

Big Data in the Cloud

The big data struggle is real, but it shouldn't deter you from embracing cloud computing. The challenge for some agencies is figuring out how to get large amounts of data from their facilities into the cloud to boost accessibility.

In response to a customer's need, DLT Solutions built a service that allows customers to send in their storage devices and have their data uploaded to the cloud. The customer receives an audited list of every file that is moved, the file disposition and whether any file is corrupted, Blankenhorn said. Collaboration between agencies and CSPs is crucial.

The work doesn't end after data migrates to the cloud. Effective management of that information is an ongoing responsibility for all parties involved and should be viewed as a journey, not a destination.

"From an acquisitions perspective, from a full life cycle, we're actually focusing on evangelism and knowledge transfer," Blankenhorn said. "So again, helping customers understand the art of the possible as it relates to cloud technology."

ABOUT DLT SOLUTIONS

For more than 20 years, DLT Solutions has been dedicated to solving public sector IT challenges. Guided by relentless focus, they have grown to be one of the nation's top providers of world-class IT solutions. Leveraging strategic partnerships with top IT companies, DLT develops best-fit solutions for customers. Their sales, integration, and support experts have the certifications and experience in helping customers at any level of any agency. DLT has both deep subject matter expertise and in-depth knowledge of government-mandated requirements and initiatives in areas such as a cloud computing, cybersecurity, and consolidation.

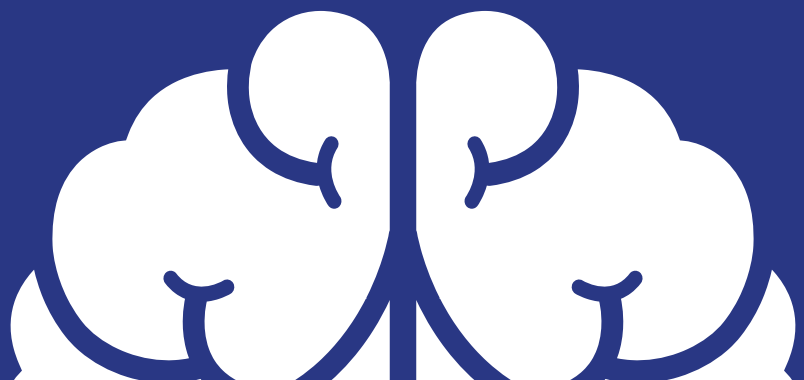
DLT SOLUTIONS®

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 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 connect and improve government.

For more information about this report, please reach out to Nicole Blake Johnson, Technology Writer, GovLoop, at **Nicole@govloop.com**.

1101 15th St NW, Suite 900 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop



1101 15th St NW, Suite 900 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop