THE FUTURE OF CLOUD

5 of the Latest Cloud Computing Trends in Government

CONTENTS

EXECUTIVE SUMMARY

In the information technology world, few buzzwords are more mystical than "cloud computing." Sure, we use the cloud to access email and work files, and to do online shopping, but most people don't consider the details of what's happening behind the scenes to give us anytime, anywhere access to data and services. We simply expect it to work.

At its core, that's what cloud computing is all about. It's a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of resources, whether they're networks, servers, storage, applications or services, according to the National Institute of Standards and Technology. IT workers can rapidly provision and release those resources with minimal management effort or service provider interaction.

Although the concept of cloud computing isn't new, the government's growing commitment to buy IT as a service is fairly new. Today, about 8.5 percent, or roughly $7 billion, of the government's IT spending goes to provisioned services such as cloud computing.

But there's still a lot of confusion around cloud procurement, implementation and security that the public and private sectors are working to clarify. And another challenge for IT departments is that cloud removes their role as the gatekeepers of technology services. The ease of buying cloud solutions has "helped transfer buying power from IT to functional lines of business like marketing, finance and operations," according to the research firm IDC.

"Security and regulatory remains the biggest barrier for cloud adoption across industries like government and financial services, while loss of perceived control over IT assets and massive legacy systems are also stumbling blocks for using cloud," IDC found.

To help agencies overcome these barriers, GovLoop spoke with public-sector IT leaders about the latest cloud computing trends that will address these issues. Much progress has been made to gain efficiencies through cloud computing, but plenty of aspects of the cloud need further development.

"In the cloud platforms that are available to us today, there are a couple of missing pieces that we still need," Federal Chief Information Officer Tony Scott said at a recent GovLoop training event. "We worked hard on the security piece, and I'm pleased with the progress there, but we also need highly scalable cloud services like workflow management and document management that we can start to build new applications on top of to displace the old legacy applications."

In this guide, we explore the future of cloud computing and what it means for government. After reading this guide, you will gain a better understanding of:

- The latest trends in cloud adoption.
- New resources for negotiating cloud contracts and service-level agreements.
- Tips for improving cloud implementation and management.
- New tools and processes to secure cloud services.
- How to prepare the IT workforce for cultural changes associated with cloud.

Whether you are a novice or more advanced in your adoption of cloud computing, there is something in this guide for everyone. Let's start with a conversation about how agencies find the right cloud model to fit their needs.

Trend #1:

SELECTING THE RIGHT CLOUD FOR YOUR NEEDS

Public-facing websites and email were among the first services governments moved to the cloud. As cloud adoption evolves, agencies are setting their sights on a host of software applications and hybrid cloud deployment models. This section will explore the latest services agencies are moving to the cloud and how they are making those decisions.

A Snapshot of Government Cloud Activity

Depending on whom you ask, moving to the cloud is a no-brainer. There are cost savings to be had, greater efficiencies and the ability to quickly respond to spikes or drops in IT resource demands.

According to the president's 2016 budget proposal, cloud computing and other provisioned services currently make up 8.5 percent of the government's more than $80 billion IT budget.

"When you think about that, that doesn't sound like a huge percentage of federal IT spending, but in reality you have to look at the growth," said Sean McCarthy, Research Director for IDC Government Insights. "It's practically doubling every day. The long-term trend is that the government has spent more on cloud computing every year than they said they were going to at the beginning of the budget year."

The majority of cloud service providers that have met the program's rigorous standards specialize in infrastructure services, said Matt Goodrich, Director of the Federal Risk and Authorization Management Program (FedRAMP). The governmentwide program is housed within the General Services Administration.

Goodrich noted that the trend for many agencies experimenting with cloud has been adoption of infrastructure services, such as website hosting or storage of public-facing data.

But the tides are gradually turning.

Based on new data FedRAMP released in August 2015, we know that there are more than 1,400 cloud implementations across government, some of which are duplicates. Overall, that number represents more than 80 different cloud services.

Those initial numbers are expected to grow as more cloud providers request to be included in the roundup, Goodrich said, noting that there's a lot of Software-as-a-Service (SaaS) that agencies are using but not reporting. He expects to see more evidence of software implementations, particularly for cloud-based communications such as unified messaging, as the initial inventory of cloud services expands.

Cloud in the Commonwealth

In Pennsylvania, moving to the cloud is not about doing it because it's popular or trendy, said John MacMillan, the commonwealth's CIO and Deputy Secretary for IT.

It's about providing a new capability that empowers employees and better serves citizens. Ultimately, customer demands from state agencies are driving cloud investments.

Pennsylvania's journey is one example of a growing trend in cloud deployment models. Increasingly, everything is moving toward hybrid, McCarthy said.

NIST defines hybrid cloud as two or more distinct cloud infrastructures (private, community or public) that remain unique entities but are bound by standardized or proprietary technology.

"For us, it's about cloud enablement, rather than specifically cloud services," MacMillan said.

A year has passed since Pennsylvania awarded a massive cloud computing contract to consolidate seven data centers into a single secure hybrid cloud. At the time, the contract was valued at an estimated $681 million over seven years, with three one-year renewal options.

"And where we are now, a year later, is starting to figure out the actual demands for some of the services that were included in the agreement," MacMillan said.

McCarthy noted, "We used to say, 'This is private, this is public and this is hybrid,' and the hybrid was the smaller of those

three groups. And what's happening is that people are realizing that in order to integrate their systems, share the data across multiple environments, sometimes across agencies, etc., it almost always ends up becoming a hybrid environment eventually."

Building Customer Relationships

The benefits of cloud computing are enticing, but not every IT system can or should be retrofitted for the cloud, said Jonathan Feldman, CIO for the city of Asheville in North Carolina. Conversations and decisions about what services can and cannot move to the cloud should include government customers who use those services. Cloud security is a key part of what Feldman calls a consultative and engaging discussion.

"Have you ever heard the expression 'Don't fall in love with the house until you move in'?" he asked. Well, the same is true when it comes to IT products and services, Feldman said.

Many times security is an afterthought because the main focus for non-IT users is whether the capability can meet their mission needs. Once they have already fallen in love with the software, it becomes even harder for the IT department to come in and voice their security concerns.

A lack of multifactor authentication, which requires more than a username and password for accessing a service, is one of the common shortfalls, Feldman said.

When speaking with IT end users, he makes it clear that as their trusted adviser, it's important to have a conversation about what happens if a provider goes out of business, has a major hack or loses all its data.

Feldman tells his staff to think of themselves as marbles. Every time they tell someone what cannot be done because of security, "we're taking a marble out of the jar," he said. Every time his team delights users with a new tool that really helps them and saves them time, marbles go into the jar.

He recommends establishing lines of communication early so that sound advice down the road doesn't fall on deaf ears.

Feldman summed it up this way: "I think an IT organization that practices extreme helpfulness is in a lot better position to say, 'Hey, did you know you're about to make a huge mistake?' and [actually] be listened to."

Remember, the more helpful you are at adding value, the more marbles you'll have in your jar.

Decision Framework for Cloud Migration

Deciding what services can move to the cloud — and when — can be challenging. When former Federal CIO Vivek Kundra released the government's Cloud Computing Strategy in 2011, he included a framework to help agencies plan for cloud migration. Below is an outline of the framework that can be adapted to meet agencies' specific needs.

FRAMEWORK IS FLEXIBLE AND CAN BE ADJUSTED TO MEET INDIVIDUAL AGENCY NEEDS

Select

Identify which IT services to move & when

Identify sources of value for cloud migrations: efficiency, agility, innovation

Determine cloud readiness: security, market availability, government readiness, and technology lifecycle

Provision

Aggregate demand at Department level where possible

Ensure interoperability and integration with IT portfolio

Contract effectively to ensure agency needs are met

Realize value by repurposing or decommissioning legacy assets and redeploying freed resources

Manage

Shift IT mindset from assets to services

Build new skill sets as required

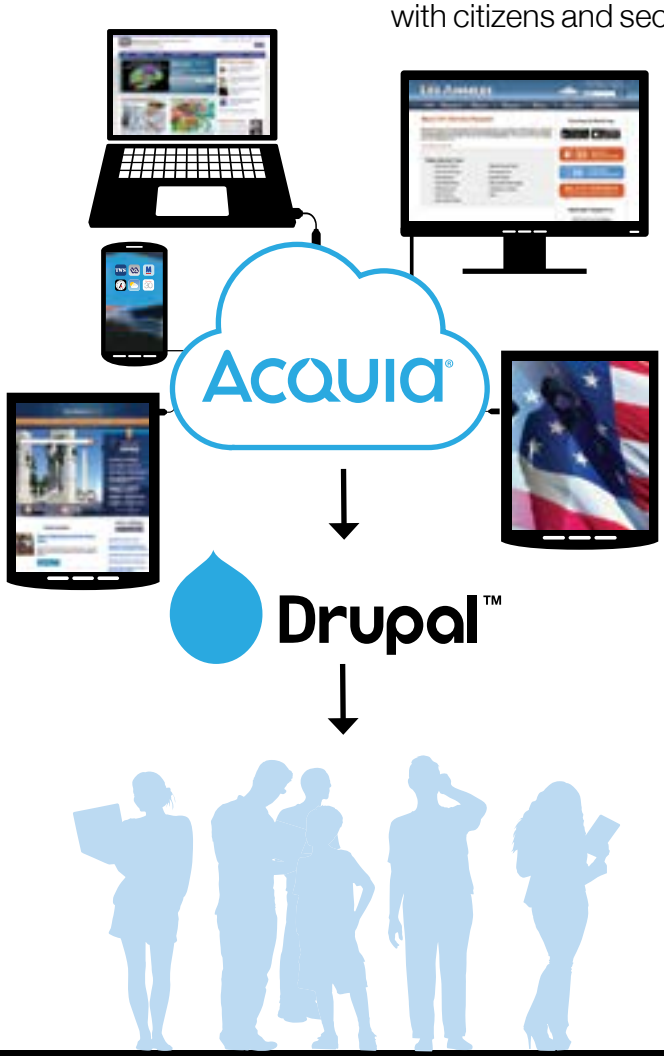
Actively monitor SLAs to ensure compliance and continuous improvement

Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Source: Federal Cloud Computing Strategy

Optimize Your Digital Web Experiences

Acquia helps agencies build, deliver, and optimize solutions on our open digital cloud platform. Built on a Gartner Magic Quadrant Leading CMS, our platform enables agencies to foster greater digital engagement with citizens and securely deliver mission essential information and services greater speed, agility, and resiliency.



Innovate with greater Speed and Agility

- → Digital Platform Optimization
- → Open Cloud Hosting
- → Drupal Migrations & Training
- → Drupal 8 Availability/Drupal 6 Support
- → Personalization and Smart Data
- → Web Content Management (WCM)
- → Professional Services & Support

STATE OF GEORGIA CASE STUDY →

CITY OF LOS ANGELES IN THE NEWS →

FEMA CASE STUDY →

AUSTRALIAN GOVT. IN THE NEWS →

To learn more visit us at acquia.com/government

or to ask us a question about our solutions and services please visit

www.acquia.com/contact-us-about-acquia-platform

CHOOSING THE RIGHT CLOUD SOLUTION FOR DIGITAL ENGAGEMENT

An interview with Dan Katz, Technical Director, Public Sector, Acquia

Cloud computing has gone mainstream, thanks in part to the rise of tech-savvy citizens who are placing pressure on government agencies to improve citizen engagement and digital services. While agencies like the Department of Interior, GSA and the White House are pioneering digital transformation and cloud-first efforts, understanding the basics of cloud computing models is still difficult for many agencies.

Government agencies have a mission and an obligation to provide information and services to citizens anywhere, anytime, on any device. Cloud models play a key role in digital web strategies and in enabling agencies to improve information delivery, provide essential citizen services and increase operational efficiency.

"The cloud service model you choose, along with the platform and service provider, also determines the resources, time, cost and level of effort an agency needs to invest in delivering great digital web experiences," said Dan Katz, Technical Director of Public Sector at Acquia. "At its core, cloud is all about paying to use someone else's resources." He offered a brief overview of three cloud service models and the investment for government agencies:

Infrastructure-as-a-Service gives agencies access to network, hardware, data center resources and sometimes operating systems through a vendor like AWS or Rackspace. If agencies want to build their own web platform, manage it, and run it, IaaS gives them the feel of having their own infrastructure that resides in someone else's data center. This option usually requires a large investment of agency time and resources, and a dedicated team to manage everything from technology updates and security monitoring to managing helpdesk tickets, scalability, and website uptime.

Software-as-a-Service is a feature-complete application you pay to let users access. Rather than the customer managing the rollout of new features and access to the application, the vendor does. The features are designed to meet the common needs of every customer, which means agencies are somewhat limited if they want custom applications to deliver customized mobile or web services. SaaS requires very little effort, but does require an investment in IaaS and/or PaaS that are managed internally or outsourced to vendors. Because these are usually managed by different entities, there is a lack of complete ownership, which can result in site downtime and other technical failures.

Platform-as-a-Service is the sweet spot, because it combines the best of IaaS and SaaS. PaaS gives customers a scalable infrastructure, a set of reusable components, a framework, a platform, and tools to build different types of apps on that platform. Additionally, unlike the IaaS model, the level of vendor support usually goes above just managing the infrastructure. Katz presents the question: "Would you rather have your IT resources keeping servers patched and updated, monitoring traffic, and supporting content managers? Or would you rather outsource that to a vendor like Acquia and let those valuable resources focus on innovation and developing new solutions and game-changing transformation initiatives? In addition, 100 percent of ownership for SLA's fall to the vendor, not the customer."

Only a few vendors, including Acquia, have created a cloud platform specifically tuned to the needs of managing digital experiences, and the results for customers have been significant. FEMA reported a 93 percent improvement in site performance, while the state of Georgia has recorded $5 million in savings, and the city of Los Angeles reported increased call center staff efficiencies due to more than 100K mobile submissions through MYLA311.com.

But how can agencies ensure the cloud model they are asking for is what they want and need? Agencies should look for cloud vendors and initiatives that align with their goals and work with them to clearly understand what tasks will be outsourced and what will remain in-house. Communication is key!

Katz also recommends that agencies move past the use of cloud computing buzzwords and focus their conversations on answering these key questions:

- What are they trying to accomplish?
- What is the mission?
- What are the business requirements?
- What is the digital transformation strategy?

If security is your concern, keep in mind that cloud providers are required to meet government security standards before they are authorized to operate within an agency. There are also ongoing requirements to ensure cloud solutions remain secure. For some agencies, cloud environments provided by vendors are more secure than their internal, legacy systems.

"Cloud providers have a lot more to lose," Katz said, noting that a breach for any vendor would be devastating for both customers and the company's bottom line.

But the truth is that much of the data agencies are worried about securing is unclassified and can be publicly released. Moving data, especially public data, to the cloud can free up internal resources and staff to do other projects.

Trend #2:

CREATING A BETTER PROCUREMENT PROCESS

Procuring cloud services has its challenges, from crafting service-level agreements to negotiating deals and ensuring an agency has covered all its bases. As agencies seek to migrate more services to the cloud, here are the best practices that are gaining steam among forward-thinking organizations and programs.

FedRAMP 2.0: Moving Cloud Adoption Forward

Buying cloud services can be easier said than done. For agencies that aren't used to buying IT as a service, uncertainties and risks abound, including how those services are secured and whether they meet government standards.

By taking the guesswork out of cloud security, FedRAMP has helped move cloud adoption forward. Agencies in the throes of cloud implementation can testify that security goes hand in hand with procurement. Security requirements help reduce uncertainties and risk and ultimately spur rapid and cost-effective procurement of cloud services.

FedRAMP was designed to speed cloud adoption by standardizing cloud security requirements. And it has quickly evolved in the past six months. Since the launch of a two-year roadmap in December 2014, the program has embarked on several new efforts to:

- Develop draft guidance for incorporating FedRAMP requirements into cloud computing acquisitions. That guidance is due October 31, 2015.
- Provide online training to increase education and awareness of FedRAMP and how it works.
- Publish practical guidance for agencies to reuse FedRAMP authorizations of cloud services that meet government standards.
- Create a crowdsourced challenge to find an open source, innovative solution to automate FedRAMP documentation.
- Coordinate with the Homeland Security Department to create cloud overlays for companies to demonstrate compliance with other IT policies, such as the Trusted Internet Connections initiative, as they complete FedRAMP assessments. The goal is to create overlays for other security requirements and standards, such as IPv6, which specifies Internet protocols for the growing number of devices connecting to the Internet, and Homeland Security Presidential Directive-12, which requires federal agencies to issue and enforce the use of Personal Identity Verification smartcard credentials to access federal facilities and information systems.

In addition to the changes listed above, check out the security section of this guide on Page 20 for FedRAMP efforts to improve continuous monitoring and define standards for securing more sensitive data in the cloud. A lot has happened in such a short amount of time, and keeping pace with these changes will help you become a more informed cloud buyer.

The purpose of FedRAMP's two-year roadmap is to increase government use of the program through education and training, improve program efficiencies by automating paperwork, and ensure that FedRAMP is adapting to meet agencies' evolving needs. Initiatives are grouped into six-, 12-, 18- and 24-month intervals.

One major milestone of the program is that the number of FedRAMP-compliant cloud providers jumped 41 percent in the past six months, Goodrich said. That number has likely grown since it was first released in August 2015.

"We were just trying to show some sort of exponential growth, and the number of providers and options available through FedRAMP," Goodrich said.

Of the more than 1,400 cloud implementations identified across government agencies, 82 percent are covered by a cloud authorization. A vast majority of the remaining 18 percent are working toward a FedRAMP authorization. The benefit for agencies is huge.

10 FACTS ABOUT FedRAMP

To better understand the current state of cloud in government and agencies' future needs, the Federal Risk and Authorization Management Program issued a request to see how many cloud services and instances of those services are in use governmentwide. The data was released in August 2015 and will be updated quarterly and parsed to identify trends.
Here are a few of the highlights:

80
the number of cloud services used in government

1,400
the number of cloud implementations, or instances of those cloud services in government

82
the percent of cloud implementations FedRamp covers

38
the number of FedRamp-compliant cloud service providers

41%
growth in FedRamp-compliant cloud providers between December 2014 & June 2015

$70,000,000
the annual cost agencies avoid by reusing FedRamp security authorizations

1,000
the number of public comments FedRAMP received on its draft standards for securing high-impact systems in the cloud

24 to 40 hours
The average amount of time it takes the Joint Authorization Board (JAB) to conduct quality reviews

500
people who have enrolled in FedRAMP online training in a five-month period

95,000
users who have visited the new FedRAMP.gov since the website's re-launch in March

dRAMP

By using FedRAMP, agencies have avoided $70 million a year in costs because they no longer have to start from scratch and reevaluate cloud providers on their own.

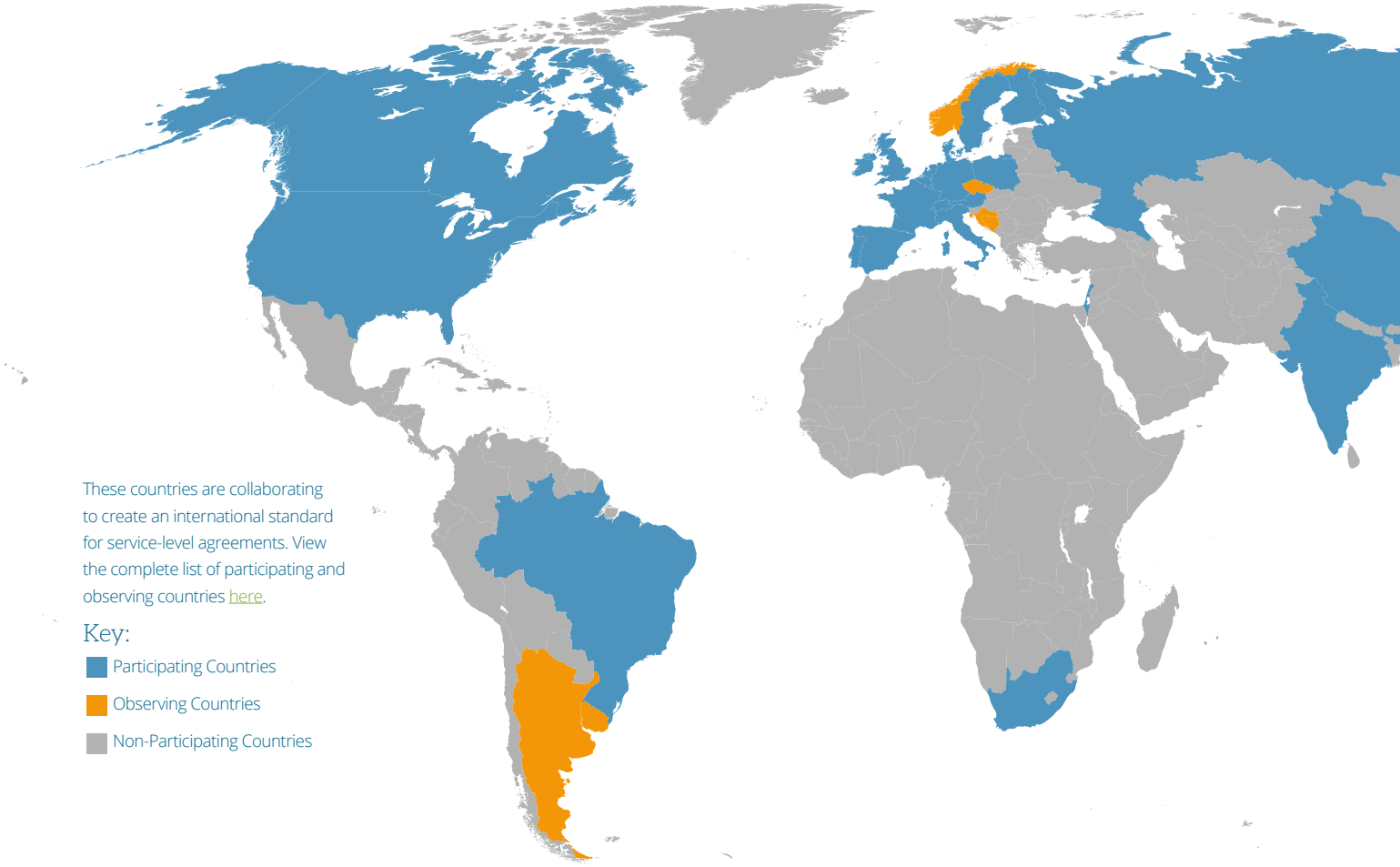
As much as Goodrich advocates for the use of cloud, he admits that cloud isn't always the answer.

"Not everything is right for cloud, but cloud is the right answer for a vast majority of things that you want to do now," he said at a recent FedScoop event. "It does require planning, and it requires making sure that you actually buy it appropriately."

In the next section we explore how strong service-level agreements help agencies buy cloud services that meet their needs and requirements.

Visit FedRAMP.gov for more insights on current and upcoming changes to the program.

ISO/IEC JTC 1/SC 38 - Cloud Computing and Distributed Platforms



Spotlight Interview

BRINGING STANDARDS TO SERVICE-LEVEL AGREEMENTS

An Interview with John Messina, Computer Scientist, NIST

Whether you're a stickler for standards or not, the U.S. federal cloud computing market is better off because of them. Thanks to FedRAMP, there are now baseline standards for securing cloud products and services in use governmentwide.

But the work doesn't end after an agency finds a FedRAMP-compliant vendor. One of the struggles governments at all levels face is articulating the level of service they expect from their cloud providers and, in turn, understanding the limitations of what can and cannot be provided.

Part of the problem is that service-level agreements (SLAs vary widely across cloud providers, and sometimes different divisions within the same company offer the government very different SLAs, said John Messina, a Computer Scientist at NIST. "The customers really couldn't compare the cloud services," Messina said. "Even if the cloud services were identical, the underlying SLAs couldn't be compared."

Customers were frustrated, uncertain and less inclined to move to cloud services because they did not fully understand the risks.

"Agencies who have not done much in cloud computing, they don't even know what questions to ask or what components should be in the contract, based on their particular business needs," Messina said. He expects that cloud adoption will accelerate as agencies gain a better understanding of what services cloud providers will and will not offer.

What agencies need is guidance. And it's coming in the form of a new international standard that 29 countries are developing. Messina is part of the U.S. group working on the standard. The group's name is a mouthful — ISO/IEC JTC 1/SC 38 — and includes representation from most of the major players in the cloud space.

The standard will include multiple parts. The first part, which will provide an overview for using common vocabulary and terminology in SLAs, will be completed in early 2016. Two other sections are slated for completion around the fall of 2016, and they will help agencies identify the major metrics and requirements that are used in SLAs. But the sections are not prescriptive.

Although the draft standard prompts agencies to address termination of service requirements and service reliability in their contracts, the standard won't specify whether agencies should request 99.9999 percent availability of their cloud service vs. 99.99 percent. These specifics will vary based on individual agencies' requirements, and remember, costs usually increase as the level of service does.

What the standard will give customers and agencies is a checklist of the major concepts that could appear within their SLAs, Messina said. "At the very least, each customer and provider should then go through this list of components and have a frank discussion on whether it makes sense for any specific contract."

The United States, China, Australia and the United Kingdom are among the 29 countries collaborating to develop an international SLA standard. Eight more observing countries are interested in the end result. Check out the map below to see which countries are participating:

SERVICE-LEVEL AGREEMENTS OF THE FUTURE

If you can't wait until 2016 to see what's included in the SLA standard, we have a sneak peek for you. The standard is currently in draft form, but here is some terminology that is likely to appear in the final version. These key terms are common in cloud SLAs, and they deal with business agreements:

Covered Services Component:

Identifies the cloud services the SLA covers.

Roles and Responsibilities:

A description of the roles and responsibilities for the stakeholders (typically cloud provider and customer).

Availability:

The property of being accessible and usable on demand. (This is where the provider would make a promise of amount or percentage of time in a given period that the cloud service is accessible or usable.)

Protection of Personally Identifiable Information:

This is where the provider would make assurances relating to the protections of personally identifiable information. Several examples include the time periods for erasing temporary files, the length of time data logs are kept and the time period notification for data breaches.

Termination of Service:

Deals with the orderly exit process when the use of the cloud service is terminated. (Elements would include notification of service termination, acceptable methods of returning assets and the length of time the vendor retains data at the end of service.)

Service Reliability:

The overall process by which reliability is considered typically consists of three parts: service resilience, customer data backup/restore and disaster recovery. (Elements include specific allowable number of service failures in a given time period, time it takes for services to recover, backup methods, period of time between backups, number of backup generations stored, etc.)

IT connects citizens and governments

BMC helps people get easy, efficient access to government services.

bmc for Digital Government

Bring IT to Life at **bmc.com/federal**

A CLOUD MANAGEMENT REVOLUTION

An interview with Herb VanHook, Vice President and Deputy Chief Technology Officer, BMC

Extolling the benefits of cost savings, the past three federal Chief Information Officers have ushered in the era of cloud computing for federal agencies. Back in 2011, the White House mandated that agencies consider cloud before all other technology solutions. But investing in the cloud and optimizing the processes and procedures in the cloud are two radically different propositions.

In order to better understand how to get the true value out of the cloud, GovLoop sat down with BMC's Vice President and Deputy Chief Technology Officer, Herb VanHook. "The initial reason most federal agencies consider cloud solutions is the promise of lower costs. While the cost efficiency of cloud can work in many cases, it does not work in every case. Sometimes, the short-term cost is attractive, but longer-term, the total cost will be greater. However, cloud computing can deliver the service flexibility and agility demanded by agencies with dynamic or sporadic technology requirements, and these capabilities can often outweigh additional cost considerations."

Before an agency invests in the cloud, VanHook suggests agencies consider three key areas:

Cost: Agencies must build a long-term cost model that considers different options (e.g., cloud-based versus traditional datacenter environments), and also addresses agency budget and procurement models.

Security Classifications: This is often the biggest barrier in "moving to cloud." The security requirements for data, applications and workloads greatly dictate where they may reside and run. For example, FedRAMP currently specifies controls for securing low-impact and moderate-impact systems in the cloud. Efforts are underway to develop requirements for securing high-impact systems.

Suitability: New system architectural models are emerging to take optimum advantage of dynamic cloud resources. Often, legacy systems have a poor fit with new cloud services, as they cannot take full advantage of the cloud features. This is a key consideration when thinking of migrating workloads to cloud.

As agencies adopt cloud-computing models, they will face new technology management challenges because cloud represents a new type of IT. One solution agencies can leverage to assist in the implementation and operations of infrastructure and platform cloud services is a *Cloud Management Platform* (CMP). A CMP can be used to build and operate a private cloud, it can be used to broker access to multiple clouds, and it can be used to govern and manage ongoing cloud services – public or private.

"Many current cloud solutions require IT staff to have programming skills, as the cloud services are typically exposed through an API," said VanHook. "However, agencies often want an easier self-service interface to cloud resources. A CMP can provide such an interface, with a catalog overlay, and a request model for more sophisticated cloud services – beyond the atomic compute and storage models you see with many cloud solutions. BMC has one of the industry leading CMP's in its Cloud Lifecycle Management solution."

"Cloud computing is not just about technology, it also means a change in existing processes and culture," VanHook explained. "By its nature, cloud computing introduces new flexible options, new models for rapid change and innovation, and demands for new skill sets with the IT staff. We have even seen organizational changes, with new emerging roles, driven by cloud adoption."

Cloud computing models often require agencies to rethink their processes because cloud actually introduces a new velocity and a new cadence. "Cloud enables things to happen faster, often so fast that they actually break existing processes. A cloud consumer at one agency recently said, 'thanks to cloud technology, we can actually get a new server in seven minutes, but for some reason it still takes me 30 days to get all the paperwork signed off.' This can indicate existing bottlenecks in change and approval processes," said VanHook.

Finally, the cloud procurement process is also creating some challenges for agencies. "Cloud computing tends to introduce new purchasing models – the "pay as you go" promise. Traditional government procurement processes, contract vehicles and budget cycles are undergoing an evolution today to embrace many of these new models.

BMC is leading the way when it comes to addressing these cloud computing challenges. BMC is also making sure cloud services it offers directly are secure and meets FedRAMP certification. "FedRAMP defined a set of security controls and a common playing field," said VanHook. "FedRAMP has forced all cloud vendors to scrutinize their security practices and improve security around their cloud services. It's caused all of us to invest more in creating secure, robust and well-managed cloud services for government environments."

Trend #3:

REFORMING & REGULATING CLOUD

Governments are moving past the hype and implementing cloud services. As with any project, there are costs and complexities that agencies must consider upfront, and there are also management responsibilities long after the service is implemented. In this section we explore how new federal IT reforms will affect cloud implementation and how federal regulations are influencing California's move to the cloud.

Federal IT Management Reforms

Change isn't easy, especially when people are involved.

It gets even harder when you add to that mix more than $80 billion worth of IT resources scattered across multiple program offices, bureaus and departments. That's how government has operated for decades.

But sweeping reforms that Congress passed in December call for an end to decentralized IT management and a more elevated role for department CIOs. The Federal IT Acquisition Reform Act (FITARA) makes clear that CIOs are responsible for reviewing and approving department IT contracts and technology components of all plans and acquisitions, including cloud computing. Better management of cloud investments is critical as more government IT services move to cloud environments.

"I think the future CIO is one who may actually own very few things, in some cases, but is a very powerful influence with agency leadership in making the right strategic [decisions] and engaging in discussions about what the future of that agency looks like with a different approach to IT," Scott said at an August 2015 MeriTalk event in Washington, D.C.

The world is digitizing, and the government has outsourced more IT assets to the cloud, Scott explained. Agencies are using shared services. In the past, internal employees ran everything, but increasingly agencies are going to depend on an ecosystem of players, including cloud service providers.

FITARA requires agencies to complete a self-assessment of their current conformity with the law's requirements and to make a plan that details how they will empower their CIOs with specific roles and responsibilities by year's end.

"There was a time, and it may still be true in some places, where the CIO was brought into the conversation about IT spend at the very last minute, or maybe not at all," Scott said. "And that is not what FITARA is about. Our expectation is that the CIO is engaged at the most strategic level with the executive management team and with agency leadership and even sub-component leadership around the design, intent and business outcome that's desired."

Here's what the Office of Management and Budget expects from agencies as they adopt FITARA:

- An implementation plan that identifies breakthrough opportunities for transformation and embraces the move to a digital government and business processes.
- Agency leadership that is engaged in the implementation process.
- CIO collaboration with Chief Human Capital, Acquisition and Financial officers, in addition to Inspectors Gener-

"I THINK THE FUTURE CIO IS ONE WHO MAY ACTUALLY OWN VERY FEW THINGS, IN SOME CASES, BUT IS A VERY POWERFUL INFLUENCE WITH AGENCY LEADERSHIP IN MAKING THE RIGHT STRATEGIC [DECISIONS] AND ENGAGING IN DISCUSSIONS ABOUT WHAT THE FUTURE OF THAT AGENCY LOOKS LIKE WITH A DIFFERENT APPROACH TO IT."

-TONY SCOTT, FEDERAL CIO

FITARA

al and others within the IT ecosystem. Does the CIO have their input?

- Relationship building between the CIOs and IT managers within their departments. Do we know who the good CIOs are and what they are doing?
- A believable plan of action that includes goals, objectives, resources, timelines, a budget, desired outcomes and metrics.

Agencies must update their self-assessments annually, starting April 30, 2016, and identify obstacles and shortcomings in fully empowering CIOs. Ultimately, deputy secretaries are responsible for the success of FITARA implementation. Success of IT programs — performance and integration — is CIOs' responsibility.

FITARA has drawn both praise and healthy skepticism from implementers and onlookers for its potential to help agencies control IT costs and boost collaboration between C-suite executives and other senior officials. But there's also the possibility FITARA will create an added level of bureaucracy and more reporting requirements that will cost money that isn't there to spend.

It doesn't help that 80 percent of the government's IT budget is tied up in sustaining legacy technology, or what is commonly referred to as operations and maintenance costs (O&M). Today, only 20 percent is spent on new development, and that trend will worsen as agencies artificially constrain their budgets, Scott said. The reasons for increased spending on O&M costs are twofold: sequestration and already tight budgets.

You can ask CIOs to save money and they will — by not spending on refreshing infrastructure, application development and the things that are easy to cut, Scott explained.

"This is not a case where you can save your way to success," he said. "We need to invest a little to get the outcomes that we want."

Spotlight Interview

THE EVOLUTION OF CALCLOUD

An Interview with Chris Cruz, Chief Deputy Director of Operations at the California Department of Technology

Chris Cruz knows better than most what it's like to be a provider and consumer of state IT services.

For more than a decade he has served in various IT leadership capacities across California state agencies, including the Food and Agriculture and Health Care Services departments. In June 2015, Cruz took the reigns as Chief Deputy Director of Operations for the California Department of Technology, where he is helping to forge a new technology roadmap, enhance existing cloud services and implement new cloud capabilities.

CalCloud, which provides the state's government agencies with on-demand access to a shared pool of compute resources, is key to California's cloud migration. CalCloud serves about a dozen state agencies, but that number is growing. GovLoop spoke with Cruz about cloud computing trends in the Golden State.

GOVLOOP: Can you tell me about California's cloud first policy?

CRUZ: The state has a cloud first policy that was published about a year and a half ago on looking at cloud in terms of Infrastructure-as-a-Service first, before you go out and pursue other third-party services. What the language of that policy basically says is that [agencies] need to look at CalCloud as an infrastructure service.

Part of that process was that when you look at new implementations, when you look at new system integrations, you have to consider our cloud process. We have the organization go through a gap analysis first, and if it's a good fit for CalCloud, then by all means [the Office of Technology Services] starts engaging the particular state customer, or county or city customer. If it's found, based on requirements, that it isn't a good fit for CalCloud, then they're free to look at other third-party services.

We're starting to lay out third-party services now. CalCloud is more than just Infrastructure-as-a-Service, but we have other vendor-hosted subscription services that we're now moving forward with. We're making some additions that are above and beyond Infrastructure-as-a-Service moving forward, to cover software and platform [services from] other third-party vendors.

The Department of Technology will start being a broker of services and really what's looked upon as a hybrid cloud.

GOVLOOP: I imagine you can definitely relate to the people that you're serving.

CRUZ: Yeah, and I think that's been a plus. I mean, because I've been a customer before [of] the department. I always say it's a different window that you look out of at the end of the day. So when I was appointed to this job, I was able to really come from the customer perspective on addressing some of the gaps in the service delivery model and how to address those to ensure that we're bringing business value.

GOVLOOP: Are you hearing from other states or cities that are looking at what you are doing in California and perhaps asking for insight?

Cruz: Yeah, actually I was on a Gartner forum last week, and I co-presented on our CalCloud policy and direction with the state of Hawaii. We've been working with the state of Hawaii — and Gartner has taken the lead for the state CIO in Hawaii — on adopting a new cloud implementation, a cloud policy and a cloud project. We leveraged a lot of the best practices and lessons learned. We've been reinforcing our security footprint through FedRAMP and NIST compliance to ensure that we have the right levels of security within our infrastructure and also with our cloud providers, in terms of how we're going to qualify and onboard them.

GOVLOOP: How do you get everyone on board with what you are doing with the cloud first policy?

CRUZ: The cloud first policy is not technically a mandate. So it's not mandated that people use our service. What we're trying to do in terms of moving forward is to listen to what the customers' concerns have been with CalCloud, and some of the things that they reported back to us were that rates were too high for initial services and there were other options that they could seek.

So we worked hard to renegotiate the current contract to drop the rates, which you'll see are more in line with current cloud providers, and in some cases cheaper. We heard that we didn't have the necessary enhanced levels of security that were required for some of the services that [agencies] provide. So now we've put a security event management system in place for CalCloud on the infrastructure side that makes us FedRAMP-compliant and NIST-compliant. So we addressed the security piece of it.

GOVLOOP: Are there any new or innovative approaches that your department is using to improve the way Office of Technology Services buys and implements cloud services?

CRUZ: One of the things we're also looking at as part of the CalCloud Infrastructure-as-a-Service offering is providing increased storage as part of this new renegotiated contract, disaster recovery and backups, in terms of tape backups. That's a big issue with security.

We're also looking at service-level agreements. We have a service-level agreement for CalCloud as an Infrastructure-as-a-Service. We're looking at modifying that SLA to meet the specific needs of customers when warranted. So we're working on that language right now with a couple of our folks that are interested in coming into the service. So service-level agreements are part of the scenario for [IaaS, SaaS and Platform-as-a-Service.]

We're also looking at streamlining our service-level catalog, to make it more menu- and private-construction driven. It's going to be like one-stop shopping that will have a menu for our Customer Delivery Division to address our clients and to ensure that they're selling them on cloud, and they're aware of all the services that we provided — some very attractive rates and really enhanced levels of security. Not only are we addressing this for our state folks, but cities and counties and municipalities.

We also brought in early users to adopt CalCloud, to talk about best practices and lessons learned. I brought in a change champion, or somebody from the business side. His name is Rob Schmidt, he's the [Agency Information Officer] at the Department of Food and Agriculture. I brought him in to get public sponsorship and for the direction of CalCloud. So we have a public advocate on the business side, [and] that's helping us sell and talk about the services that we're putting together.

I found that created a lot of synergy when we did that a couple months ago, when I came in this role. We have an end user group now that's been adopted — early providers to help us make recommendations on how we can continuously improve our services. That's all part of CalCloud, bringing in early adopters, bringing in folks into the end user forum that can make changes to improve the service, bring in a change champion in at the executive level. We want to make sure that our message is synchronized from the executive level all the way down to our professional staff.

Sometimes the technology's the easiest part of this equation. It's the people and process part that you need to define and ensure that you have roles and responsibilities and set expectations for. I can tell you that that's the most difficult side of this transition.

Hitachi Data Systems Federal | Alliance Technology Group

HITACHI
Inspire the Next

Hitachi Unified Compute Platform

Where efficiency and reliability ***converge***

- The most ***advanced*** converged IT and cloud infrastructure

- **HDS Federal**
  Ensures that data empowers agency missions

www.hdsfed.com

Alliance Technology Group, LLC | Brent Van Scyoc | Brent.vanscyoc@alliance-it.com | (410) 712-0270

CLOUD COMPUTING MADE EASY

An interview with Chris Williams, Vice President of Alliance Technology Group's Infrastructure, Platform, and Application as a Service Division

Easy and cloud are two words people don't often use in the same sentence, unless they're talking about the long-term benefits of cloud adoption.

The end result for many cloud adopters is cost savings, better use of existing personnel and financial resources, and less hassle planning for IT needs down the road. But in between the decision to move to the cloud and the end state is the journey. For some agencies, the greatest challenge is figuring out where to start. But what if the path to cloud was an easy one — from start to finish? Chris Williams, Vice President of the Alliance IPA Division, believes it can and should be.

"Alliance is in the business of making IT easy and consumable, and our goal is to essentially be the easy button for cloud," Williams said. "We want our customers to be able to deploy functional clouds in days and weeks, not months and years, and make those clouds easy, fast, efficient, scalable and elastic. We provide customers with the agility and control that they're looking for in the cloud."

The types of customers Williams sees moving to the cloud are new organizations, those that have new projects, or a software development requirement for agility and continuous development and integration.

"We're seeing some customers come to us looking for alternatives to some of the major public cloud providers," Williams said. "We also see many traditional organizations that are looking for ways to deliver private cloud services to internal customers with the same level of agility that's offered in the public cloud."

Alliance is all about providing agencies with the fastest and easiest path to the cloud by taking the best that the open source community has to offer and combining it with best-in-class hardware and service support. Although much of the general conversations around cloud focus on public and private proprietary cloud deployment models, open source clouds are gaining traction in government.

In 2010, NASA and Rackspace released two pieces of software into the open source community, which became the foundation for what is now known as OpenStack, Williams said. OpenStack provides an open source and transparent alternative to a lot of the proprietary cloud platforms on the market today. Since its introduction, OpenStack has seen an unprecedented level of adoption and traction in the market. Most IT vendors are now supporting it through their participation in the OpenStack Foundation, by contributing code, and ensuring their products can integrate with the open source cloud platform.

"We went from mainframes to client server, and now we're going from client server to cloud," Williams said. "For the first time in the history of IT there is not only a viable, but a very vibrant, feature-rich, open and transparent option. "That really has never been the case."

What sets open source clouds apart from proprietary clouds is the unprecedented level of transparency. Open source clouds are developed by a collaborative group of thousands of individuals and hundreds of companies representing numerous countries. They're all working together to build the best cloud framework.

Prior to government cloud adoption, standing up IT infrastructure was somewhat cumbersome. Agencies had to request networks, undergo a change management process, install operating systems, rack and stack servers and power them on. Each of those tasks represented a delay that a business unit experienced from the time they acquired equipment to when it was actually available for use, Williams said. The process to scale out that infrastructure to meet increased demands was also very slow.

But cloud service providers have proven there is a new way of doing business with agile infrastructure that can quickly meet agencies' IT needs. "Along with that, cloud has opened up a lot of new possibilities and some outcomes that I would say were previously unachievable," Williams explained.

For example, "I can now develop applications that are aware of the underlying infrastructure layer that can request additional resources on demand, without requiring administrator intervention."

Today, Infrastructure-as-a-Service providers dominate the government's pool of FedRAMP-approved vendors, but Williams believes Platform-as-a-Service is the next step for agencies that were early adopters of IaaS. "The only reason I think we don't see more PaaS adoption today than we see IaaS is because of market maturity and frankly the maturity of a lot of IT shops and where they are on their cloud journey," he said. "But PaaS is certainly catching on and picking up steam."

Trend #4:

A MORE SECURE CLOUD

One of the main concerns agencies often cite for not moving to the cloud is security. The truth is entrusting cloud providers with your data can be scary, but some commercial cloud vendors enforce tighter security measures than agencies. At the center of cloud security talks is the governmentwide program FedRAMP. In this section we discuss what the evolution of FedRAMP means for cloud security in the future.

Moving Cloud Security Forward

Security in the cloud doesn't stop after companies prove they meet government requirements. In fact, that's just the beginning. A key component of FedRAMP requires vendors to continuously monitor the security of a cloud service after it's approved for use by the government.

At a minimum, cloud providers are required to generate monthly vulnerability scans for their government customers that show any attacks or indicators of potential attacks against information systems, plus other key metrics that FedRAMP outlines. That doesn't mean government agencies are off the hook. Agencies have several responsibilities for making continuous monitoring a success, including:

- Notifying cloud providers if they become aware of an incident that has not yet been reported.
- Providing a primary and secondary point of contact for cloud providers and DHS' U.S. Computer Emergency Readiness Team (US-CERT).
- Notifying US-CERT when a cloud service provider reports an incident.
- Working with cloud providers to resolve incidents and provide coordination with US-CERT, if necessary.

The government is also responsible for ingesting and analyzing all the data that vendors provide in their monthly vulnerability scan reports. Much of that work has fallen on the shoulders of the FedRAMP Program Management Office (PMO). Here's why: The agency that works directly with a cloud provider to become FedRAMP-compliant is then responsible for overseeing continuous monitoring activities. Currently, most of those vendors have worked directly with FedRAMP's JAB to undergo the vetting process, which means continuous monitoring oversight falls to the program office.

(*Visit the resources page at the end of this guide for FedRAMP terms and definitions.*)

The intent of FedRAMP was never for one agency to carry the burden of overseeing a vendor's continuous monitoring activity and compliance on behalf of the entire federal government. Not only are the tools required to manage that task very powerful and complex, but there's also the challenge of collecting, analyzing and comparing continuous monitoring data over time to identify trends.

That's why the FedRAMP PMO is considering expanding its role to take on the continuous monitoring responsibilities for all FedRAMP-compliant services used by multiple agencies, said FedRAMP Director Goodrich. Whether this actually happens will depend on the success of an upcoming pilot to test the feasibility and scalability for the PMO to take on this expanded role. The pilot will launch in the next six months with up to five agencies.

Not only would agencies see their burden reduced, but it would also give the PMO a more holistic view of security across all FedRAMP-compliant cloud providers. When a vulnerability is discovered, the PMO can more easily check for similar security gaps across other cloud solutions.

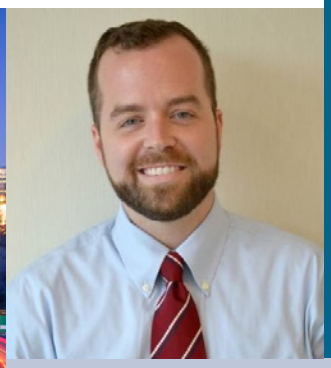
Cloud providers want to introduce changes to their environment, most on a monthly or weekly basis, and those changes must be documented and monitored for security vulnerabilities.

"The process we have now works, but it's very document-heavy and manual," Goodrich said of the continuous monitoring process. "We want to figure out how to change that and make it more scalable, particularly for providers and agency consumers who want more services."

Continuous Collaboration

Another approach to improving the continuous monitoring of cloud services involves better collaboration among customer agencies. Today multiple agencies use the same cloud solution offered by the same cloud vendor. But there is little collaboration among those agencies when it comes to monitoring cloud security over time.

FedRAMP
Federal Risk Authorization Management Program



"AS WE HAVE PEOPLE USING THE SAME PROVIDER AND THE SAME SERVICES, THE GOVERNMENT HAS GOT TO COLLABORATE. WE HAVE TO WORK TOGETHER, AND THIS IS TRYING TO GET THAT FRAMEWORK SO WE CAN DO IT SUCCESSFULLY."

-MATTHEW GOODRICH, FEDRAMP DIRECTOR

The government needs to speak with a collective voice when doing continuous monitoring so that cloud providers can talk to one group, Goodrich said. His team is developing a methodology that defines how that could work.

"We plan on identifying those that would be most beneficial [and] to launch those collaboration groups over the next six months," Goodrich said. The first step is creating a guide on how to manage so-called multiagency continuous monitoring. In a recent snapshot of FedRAMP's progress during the first half of this year, the PMO notes that "collaborating in this way gets to the heart of our 'do once, use many times' framework." Through these collaborative groups, agencies can work with cloud providers in one setting, and providers can more easily address any agency concerns.

"As we have people using the same provider and the same services, the government has got to collaborate," Goodrich said. "We have to work together, and this is trying to get that framework so we can do it successfully."

Securing High-Impact Cloud Systems

Until now, the focus for government has been moving low- and moderate-impact systems to the cloud. These are the systems that would have some, but not a drastic, impact on government operations if they were unavailable for use.

But growing demands from agencies have prompted the FedRAMP PMO to draft baseline standards for securing high-impact cloud systems, or those systems that are necessary to support agencies' continuity of operations.

The fact that agencies are even considering moving more sensitive systems and data to the cloud can be hard to wrap one's head around because government tends to be risk-averse. But the promise of on-demand IT resources and cost savings make cloud computing an attractive option for the government. Collectively, the Defense, Justice, Homeland Security, Veterans Affairs and Health and Human Services departments represent 75 percent of the market for high-impact systems.

Draft FedRAMP high standards were released in January 2015 and they garnered more than 1,000 public comments. The FedRAMP PMO has invited government employees and contractors who work on high-impact systems to join its tiger team and help adjudicate the comments. One of the biggest differences when it comes to securing high-impact systems is the increase in automated processes.

"The biggest element is trust between a cloud provider and the government to be able to share that information more readily, which is something that I think both sides need to work on," Goodrich said about the draft standards, which are expected to be finalized by year's end.

In the mean time, the FedRAMP JAB is working with four cloud service providers to pilot the high baseline standards while they are being finalized. "That way, we aren't just dealing with [it] academically, but we're also looking at it from the perspective of actually answering those questions and putting it into reality," Goodrich said about the pilot.

The pilot will also help FedRAMP officials determine if logical or virtual separation of government data from other customers' data in the cloud is possible, rather than having to physically put government data on different machines.

"That's one of the things that I think a lot of people are concerned about, and I think we're going to be proving, through this [pilot], whether or not that's actually capable," Goodrich said.

Spotlight Interview

SIMPLIFYING CLOUD SECURITY

An Interview with Michaela Iorga, Senior Security Technical Lead for Cloud Computing at the National Institute of Standards & Technology

The world of cloud computing may seem like uncharted waters for agencies that are used to seeing and touching their servers and securing their own systems. But thanks to governmentwide requirements set by FedRAMP, there's a lot more trust in cloud security than there was when the program first launched in 2012.

Still, there's more work to be done.

"FedRAMP does a great job assessing a provider's implementation of baseline security controls, but the baseline controls cover only minimum security requirements," said Michaela Iorga, Senior Security Technical Lead for Cloud Computing at NIST. "FedRAMP sets the baseline requirements using NIST standards (FIPS) and specifications (NIST SP)."

Iorga explained the challenge this way:

"The main problem with adopting cloud solutions is similar to the problem that we all have. We always trust more what we are doing with our hands than what we get from others, or expect from others. Transitioning from using in-house computing resources to leveraging computing as a utility comes with this inertia on accepting the change or understanding and trusting the new concept.

"So there are many, many facets of this diamond, since cloud computing is a new, resourceful technology. Organizations can achieve, when the cloud-solution is well implemented, a more resilient, better performing solution at a much lower cost than an in-house solution. Assessing the variety of services offered by cloud providers is an important step in adopting a cloud-based solution. You don't just go in the market and buy a diamond just because it sparkles, because it can be a Swarovski crystal. You need to be able to certify the diamond. You need to make sure the diamond you have in your hand is exactly what you are looking for."

Agencies want to ensure that they are getting at least the same level of security and services — if not better — when they move to the cloud. They know the standards and requirements for systems in-house, under their purview. If those systems are migrated to the cloud, they must still provide the same security posture, Iorga said. Part of the challenge is knowing how to orchestrate a secure cloud ecosystem that meets the agency's requirements.

NIST provides a methodology for orchestrating a cloud ecosystem in NIST Special Publication 500-299: Cloud Security Reference Architecture, and the agency is also working on NIST Special Publication 800-174. The document, titled Security and Privacy Controls for Cloud Based Federal Information Systems, is still under development and has not yet been released.

To help agencies practically apply these documents, NIST is developing a new prototype tool called the Cloud Security Rubik's Cube (CSRC). The tool will allow agencies to select their desired cloud capabilities from a comprehensive list and analyze and visualize the associated controls for securing low-, moderate- or high-impact systems.

"If I'm a government agency and I want to have control over those capabilities, I will select an architecture that gives me that control," Iorga said.

Early on, many agencies defaulted to using IaaS because it gave them more control, she added. Iorga and her team are developing

the tool for any agency that is considering a cloud-based information system solution.

Iorga said her team worked closely with the government's Federal Information Security Management Act (FISMA) experts to determine what security controls make sense to implement, based on what cloud capabilities agencies want, what data will be in the cloud and what the requirements are for securing that data.

The goal is to empower agencies and simplify the complexities of cloud computing implementation. Iorga wants agencies to be more educated when they approach cloud providers.

"We are helping government agencies to have tools, methodologies and information that they can use during their selection of the providers [and] negotiation of what they need to what is important for them," Iorga said.

The CSRC tool aggregates not only the security controls identified by the NIST team but also reflects the FedRAMP and FedRAMP Plus baselines. FedRAMP Plus is "the concept of leveraging the work done as part of the FedRAMP assessment, and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements," according to DoD's Cloud Computing Security Requirements Guide.

How the tool will be provided to agencies has not yet been determined. One possibility is putting the tool and data in the cloud, but the risks must first be considered. The information can be also shared as a large spreadsheet, but agencies will miss the benefits provided by the CSRC, Iorga said.

NIST is also developing guidance for applying the Risk Management Framework to cloud-based federal information systems. NIST Special Publication 800-173 takes the steps of the risk management framework, which includes categorizing a system, selecting security controls, implementing those controls, assessing the controls, authorizing the system and monitoring to ensure the controls are in place.

"As owners of the data and consumer of the cloud service, agencies need to have the vision of the entire ecosystem and clearly understand the roles and responsibilities of each cloud actor, and what it is they inherit from the cloud provider or broker in order to build trust," Iorga said.

Agencies must also ask:

- How well or how much do you trust what you are inheriting from the provider?
- What's the risk?
- What's the tolerance that you have toward that particular risk, based on the system that you're architecting?
- What's the residual risk that you can assume?
- What happens if something goes wrong, such as a security breach?

Before agencies sign on the dotted line of a service-level agreement, it should be clear to everyone what they are getting from the provider, including security features, and what agencies must implement themselves.


WE BRING THE CLOUD TO YOU
When it Comes to Cloud Computing... One Size Does *Not* Fit All
ViON works with you to understand your unique requirements; architecting the right cloud solution, best deployment option and service model, at a scalable consumption based cost.
Find out more at www.ViON.com or download our whitepaper on the Benefits of Cloud.
Hitachi Data Systems Federal
ViON
Building your enterprise solutions

MOVING FROM CAPEX TO OPEX IN THE CLOUD

An interview with Ray McCay, Vice President Solutions Strategy at ViON

The average government IT executive is not overly concerned about the technical nuances of what is or is not considered cloud computing. While the National Institute of Standards and Technology certainly has provided the technical definition, it's the business outcome that is most important.

The focus for IT execs is on getting employees and agency customers what they need, when they need it, and leveraging the cloud IT model to make that happen, said Ray McCay, Vice President Solutions Strategy at ViON. And perhaps the most important is the concept of when they need it, McCay stressed.

The biggest challenge is meeting those needs when there is little to no capital budget (CapEx) available to fund new projects. Most of the government's IT budget is currently funding legacy applications and systems that keep agency operations running, but doesn't provide funding for new innovations, better efficiencies, or cost savings. CIOs often refer to this way of operating as simply paying to "keep the lights on."

As older workers retire, agencies are losing the skill sets required to run the infrastructure in their data centers, McCay said. "And quite frankly, that's not what's needed from their IT organizations anyway. What CIOs have to do to add value is be responsive to the business requirements. At the end of the day, what they need is a different business model."

They need an operational expense, or OpEx, model that allows them to shrink spending if demands for IT resources shrink and increase spending if demands grow. "CIOs need to be able to quickly respond to a customer's requirements — almost anticipating what their customers are going to need and having it in place before the customer even tells them," McCay said.

The dominant Cloud OpEx model allows agencies to pay for the amount of IT infrastructure that they have access to (provisioned) on a monthly basis, but this arrangement technically does not enable agencies to pay only for what they actually use. Much less prevalent is another model that offers just that — a way to pay only for the resources that are used (within the larger amount of resources that are provisioned and available). This second approach substantially increases an agency's ability to leverage the cloud model to achieve mission success.

At ViON, the company provides a virtualized infrastructure platform that can capture how much of the environment is actually being consumed and then bill agencies only for that consumption. This consumption-based pricing is available to agencies with private cloud and hybrid cloud deployments.

When asked why more agencies aren't receiving this type of service from other vendors, McCay said, "It's an awareness issue."

"You can't ask for something you don't know exists," he added.

As agencies move more of their IT resources to the cloud, they must also consider that all clouds are not created equal. Depending on the solution, different clouds have different characteristics, they perform differently and the availability of the cloud service for agency customers may vary. Plus, not all applications can function properly in many of the typical public cloud environments available today.

One misconception McCay often hears is that some applications are very demanding and too tough to manage in a cloud environment. But that needs to be clarified.

When it comes to cloud computing, one size does not have to fit all, and there is a cloud model that can meet even the most demanding business challenges agencies face. While commodity, public clouds are a good fit for some government applications, that's not the case for all of them. "You have to make sure you understand your application, your environment, your needs, and then you pick the right architecture to solve your problem," McCay said. "Agencies shouldn't rush to the cloud without considering these things."

He encouraged agencies not to lose site of why they want to move to cloud in the first place. "There's a reason why you want to move to the cloud – not because you want to follow the crowd but it's because you need a different business model," McCay said. "You need to move to OpEx, you need to move to consumption-based pricing, you need to be able to flex your spending up and down, you need to be able to augment your staff, and you need to spend your time on other things. But you also need to run your applications and achieve mission success while you do it!"

It really comes down to the business strategy. Agencies have to figure out what it is they need, what they can afford, and how they want to pay for it – through an OpEx or a CapEx model.

Trend #5:

CLOUD'S IMPACT ON A CHANGING WORKFORCE

Migrating your IT assets to the cloud is as much a cultural change as it is a technological one. As governments shift more services to the cloud, leaders must clearly communicate any changes to their IT workforce and explain how their roles and responsibilities will evolve.

Simplifying Cloud Security

When was the last time you sat down with your boss and discussed your short- and long-term career goals? If you're a manager, has it been awhile since you asked your team members about their future aspirations and helped them navigate the career ladder?

I'm not talking about waiting until the annual review to have these discussions; that may be too late. For the IT workforce, these are critical conversations that should be initiated and revisited long before there are major changes — such as moving applications and services to the cloud. Feldman, Asheville's CIO, explained the workforce issues that IT leaders must address going forward as cloud adoption increases.

"The leaders have not necessarily been discerning about what they're choosing, [and] they're not making it clear to staff that they're valuable and they have a role," Feldman said. "People are not stupid, and they know that cloud is outsourcing 2.0, and they don't want to be outsourced."

The solution? "You've got to give people a path forward," Feldman said.

For some of Asheville's senior IT infrastructure experts, that path forward includes a revised list of professional goals, one of which is obtaining an Amazon Web Services (AWS) certification. With the certification comes valuable teachings on how to manage and maintain an AWS infrastructure, which the city relies on to run cloud applications, Feldman said.

But who pays for this professional development?

"If there's a business objective, I better darn well be willing to put some money into it," Feldman said.

When it comes to the workforce, it's about more than a certification, he added. "It is the identification of a skill set that will be needed in the future. It's a way of mapping out a path forward because all employees want is a path forward."

It all boils down to leadership and transparency. Feldman offered these words of advice for agencies as they prepare their IT workforces for the future of cloud computing:

- You can't build a high-performance culture or team unless you start looking at people as human beings and not as cogs.
- It isn't a workforce problem if leaders fail to mention there is a plan for IT employees as more hardware and software applications move to the cloud. That's a leadership problem.
- Not everyone will understand or "get" cloud. You have to give people discretionary time to tinker with the technology in an environment where failure is an option.
- If you make decisions based on technologies and not on people, you will make the wrong decisions.

Workforce Innovation in the Cloud

One of the perks that make cloud computing attractive to government is the way it allows employees to work from anywhere, at anytime and on any device. Applications, IT systems, work documents and other resources are now stored centrally in the cloud and available for everyone to consume.

What if this same cloud model could be applied to the government workforce? Let me explain. Today, government agencies all vie for talent to work on projects big and small. Amazingly talented people are working throughout government, but organizational silos have limited the government's ability to take advantage of that existing wealth of talent.

Maybe a small project requires digital services expertise for a few hours a week or a short-term assignment could benefit from the knowledge of a skilled federal worker. Think of all the time and resources you could save by pulling from existing in-house talent. That's the potential of GovCloud, a new model for developing an agile federal workforce.

"Specifically, the GovCloud model features workforce development through cloud-based skills deployment," said Melissa Kline Lee at the Office of Personnel Management. "In this model, employees are treated as an agency asset who can be detailed to organizational components on a project-by-project basis to build experience in cross-organizational work and address critical skills gaps. GovCloud employees may work on one project at a time or work on multiple projects at once, all the while building key skills in cross-organizational collaboration and teamwork."

Don't let the name fool you. Although cloud-related projects are ripe for this type of cross-agency collaboration, GovCloud projects don't focus solely on technology.

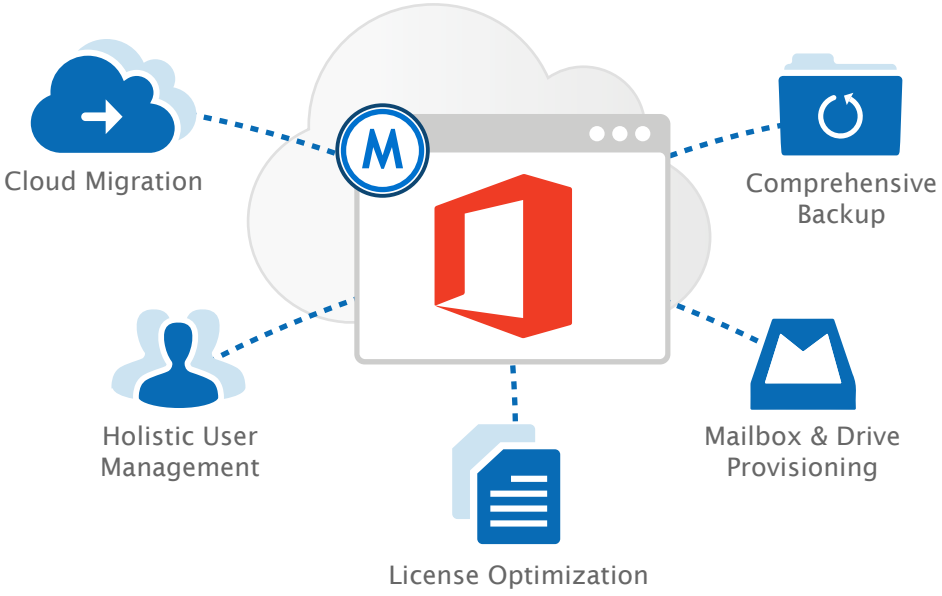
"While we are still in the design and pilot phase and cannot yet report our findings, the Department of State and the Government Services Administration have GovCloud models that are showing promise and demonstrating results," Kline Lee said.

GovCloud is one of three workforce agility-models that agencies are testing this fiscal year and next. These models fall under a larger umbrella program known as GovConnect.

"The goal of GovConnect is to develop federal workforce skills through cross-agency collaboration and teamwork, to enable more agile response to mission demands without being unnecessarily limited by organizational silos," said Kline Lee, who serves as Program Manager of GovConnect. "As part of the President's Management Agenda, the Office of Personnel Management and Environmental Protection Agency are using the GovConnect pilot to help agencies test and scale new approaches to workforce development. The learnings from this pilot will help build a 21st-century civil service that can better respond to mission demands, as well as handle cross-agency program and policy challenges."

Check out this 2014 memorandum to learn more about GovConnect's objectives and proposed methodology.

Metalogix



Moving to Office 365?

Metalogix Essentials Makes it Easy.

Metalogix Essentials for Office 365 makes it simple to move to the Cloud. With one installation, it provides everything you need for complete lifecycle management of your Office 365 environment. One unified platform provides a secure and efficient deployment from onboarding, day-to-day user and environmental analysis, to optimization, security, and backup/restore operations.

Metalogix Essentials for Office 365 helps ensure your Office 365 migration goes smoothly while reducing the administrative workload of ongoing management. Don't just take our word for it, judge for yourself.

DOWNLOAD A FREE TRIAL NOW

REQUEST A DEMO:
Metalogix Essentials for Office 365

www.metalogix.com/essentials

EASING CLOUD MIGRATION

An Interview with Dr. Steve Marsh, Senior Director of Product Management and Marketing, and Pat Park, Regional Vice President of Public Sector, Metalogix Software

The great cloud migration in government is well underway. How various government agencies support the cloud will differ depending on whether the agency is federal, state or local. For example, most federal agencies, like the Department of Defense (DoD), would be less likely to transfer everything to the cloud due to the department's extensive storage of classified information.

GovLoop spoke with Steve Marsh, Senior Director of Product Management and Marketing, and Pat Park, Regional Vice President of Public Sector, from Metalogix, to discuss why government agencies should join the cloud migration and how Metalogix can help ease the transition.

For over a decade, the company has developed trusted management tools for cloud-based platforms like SharePoint and Office 365. The company helps public and private sector organizations monitor, migrate, store, synchronize, archive, secure, and backup collaboration platforms.

For any skeptics out there, it may be important to first address **why should government agencies adopt cloud solutions?**

Aside from keeping up with the times, the primary benefits of cloud migration and deployment are cost efficiency and improved security.

"It's the ability to cut costs from servers, applications and storage," Park said. "You're paying for what you already use. As for increased security, you don't have to worry about things not being up to date in your system, allowing for potential breaches."

An inadvertent way of enhancing cybersecurity through the cloud is combatting Shadow IT. "If the tools and platform provided by the agency aren't working the way people want them to work, employees will find their own way of doing it," Marsh said. "OneDrive can stifle shadow IT because it provides a simple, easy way to upload content to the cloud and share it with multiple people."

Additionally, it's easy to navigate both worlds: the cloud and on-premise. "Your new and old applications can coexist," Park said. "You can have Exchange, SharePoint, or file shares on-premise and the same solutions on the cloud side. You'll still have the capability to communicate and operate in both worlds."

Finally, cloud helps government keep in touch with younger citizen bases. "You've got to straddle both worlds," Park said. "The concern with government agencies and the growing number of retirees is that you have younger people who grew up with all this technology. Technologies like the cloud need to be in place for them to work and operate."

Plan. Migrate. Manage.

Metalogix helps agencies formulate a migration path and prioritize a plan for moving to the cloud. "It's really about making sure you have the strategy first. Think about what you actually have as an organization and how you're going to implement it," Marsh said.

The company emphasizes helping agencies with an easy, less time-consuming migration to cloud deployment with the following steps:

- *Plan: Pre-Migration.* Metalogix tools help you to prepare and plan for a successful migration with its Essentials, Content Matrix and Migration Expert solutions. These can help your agency analyze, find and fix potential roadblocks.
- *Migrate: In one Hop.* Metalogix helps your organization directly migrate from older SharePoint versions to SharePoint 2013 or Office 365 in one go. Intermediate SharePoint versions aren't necessary to migrate your libraries, workflows, permissions, meta-data, or version history.
- *Manage.* Run old and new versions in parallel and test and rearrange your platforms as often as needed. Content Matrix is licensed to allow unlimited testing, reorganization, and management of sites and content on the cloud.

Benefits of the Cloud

The advantages to cloud deployment far outweigh the disadvantages. The only real downside is work can become your whole life. "You can work anywhere in the world once you get into the cloud," Park said.

Another important benefit includes increased storage for your agency. "One of the biggest advantages is OneDrive and the amount of storage for agencies to use that's already paid for," Marsh said.

The cloud is here and it's not going away. How will your agency start planning its migration? Because, as Marsh concluded, "Cloud is not an if, it's a when."

WHAT'S NEXT FOR CLOUD?

The next six to 12 months will be an exciting time to watch the evolution of cloud standards and how they spur greater adoption among government agencies. NIST, FedRAMP and even international groups are diligently working to provide better guidance for executing cloud procurements and enforcing security requirements.

"The new architecture that I think we have to have as we move into this cloud area is secure by design," Federal CIO Scott said. "Security will be built into every layer that works together to protect the information and the assets in that environment."

Think of all the applications that power the public and private sectors. Most of it is technology architecture that is more than a decade old. "What's happened is we've tried to slap on security and bubble wrap," Scott said. Among his priorities is working with the private sector and standards working groups to create architectures that are secure by design.

Better security in the cloud starts with agencies knowing what they already have. At the federal level, OMB is working with agencies to improve its data collection processes and better track cloud investments.

Specifically, OMB is revising the questions it asks agencies. In the past, it asked only basic questions to find out whether agencies were using cloud. OMB is now refining its methodology to get more specifics about agencies' cloud investments.

"I think we're seeing much more interest in SaaS kind of things," Scott said. "There was some uncertainty of whether you count that as cloud."

As agencies add SaaS and PaaS to their catalog of cloud services, they must also coordinate with end users and IT staff to work through cultural changes. For employees, there's the angst of learning how to use a new system. IT staff must get used to management of virtual assets instead of physical hardware.

"You have to allow experimentation, and it's like anything else in life," Scott said. "You have to begin to exercise the muscle before you can use it fully."

RESOURCES

OVERVIEW AND ISSUES FOR IMPLEMENTATION OF THE FEDERAL CLOUD COMPUTING INITIATIVE

Congressional Research Service, 2015

Research report on cloud computing and its implications for federal information technology reform management

FEDERAL CLOUD COMPUTING STRATEGY

Vivek Kundra, Former U.S. Chief Information Officer, 2011

Federal strategy outlining the benefits, considerations, and trade-offs of cloud computing, as well as a decision framework to support agencies' cloud migrations

FEDRAMP FORWARD

FedRAMP Program Office, 2014

Roadmap outlining key FedRAMP priorities for the next two years

FEDRAMP COMPLIANT SYSTEMS

FedRAMP Program Office

List of the FedRAMP- compliant cloud systems that have been approved for government use

DOD APPROVES 23 COMMERCIAL CLOUD SERVICE OFFERINGS

Defense Information Systems Agency, 2015

New release announcing vendors that have met FedRAMP moderate baseline standards and are approved to host DoD's non-controlled unclassified data

INFORMATION ASSURANCE SUPPORT ENVIRONMENT (CLOUD COMPUTING)

Defense Information Systems Agency

Website provides a knowledge base for cloud computing security processes in the DoD and cloud service provider security requirements

THE PRESIDENT'S BUDGET FOR FISCAL YEAR 2016 (INFORMATION TECHNOLOGY)

Office of Management and Budget, 2015

Background information on current and future IT investments from the president's budget

MANAGEMENT AND OVERSIGHT OF FEDERAL INFORMATION TECHNOLOGY

Office of Management and Budget, 2015

Memorandum outlining implementation guidance for the Federal Information Technology Acquisition Reform Act (FITARA)

NIST CLOUD COMPUTING SECURITY REFERENCE ARCHITECTURE

National Institute of Standards and Technology, 2013

Draft document outlining security for cloud computing in the federal government.

ABOUT GOVCONNECT

Chief Human Capital Officers Council

Objectives and proposed methodology for the GovConnect program

FedRAMP Terminology

Joint Authorization Board: The program's primary decision-making body is the Joint Authorization Board (JAB), comprised of the Chief Information Officers from the General Services Administration, Defense Department and Homeland Security Department. In addition to the JAB, the Office of Management and Budget, the Federal CIO Council, the National Institute of Standards and Technology, DHS, and the FedRAMP Program Management Office play key roles in effectively running FedRAMP.

Authorization to Operate: An agency's formal declaration that authorizes operation of a cloud product or service and explicitly accepts the risk to agency operations. An ATO means the system has met and passed all FedRAMP requirements to become operational.

Provisional Authority to Operate: An initial approval of a cloud service provider's authorization package by the JAB that an executive department or agency can use to grant a security authorization and an accompanying ATO.

Third-Party Assessment Organizations (3PAOs): Perform initial and periodic assessment of cloud service provider systems per FedRAMP requirements, provide evidence of compliance and play an ongoing role in ensuring that providers meet requirements. There is a formal application for becoming an accredited 3PAO.

Continuous Monitoring: After a system receives a FedRAMP authorization, it is probable that the system's security posture could change over time due to changes in the hardware or software on the cloud service offering or due to the discovery and provocation of new exploits. Ongoing assessment and authorization provides federal agencies using cloud services a method of detecting changes to the security posture for the purpose of making risk-based decisions.

DLT.COM

ENTERPRISE VAULT FOR AMAZON WEB SERVICES:

Making new headlines in government email management.

Meet upcoming Capstone requirements for Public Sector

A one-of-a-kind cloud-based, innovative solution to email archiving and records management built and implemented by DLT

Store, Manage and Discover unstructured information built on a FedRAMP-compliant infrastructure-as-a-service (IaaS) cloud

Available on a variety of cloud-friendly procurement vehicles, including GSA IT Schedule 70, NITAAC CIO-CS and SEWP V

amazon web services | Partner Network
PREMIER CONSULTING PARTNER

Symantec.
VERITAS

DLT

THE FUTURE OF HASSLE-FREE EMAIL INQUIRIES IN THE CLOUD

An interview with Greg Agana, Senior Engineer and Technologist, DLT Solutions

In recent years, the issue of congressional inquiries has become an increasingly hot-button issue, with everyone from Senators to presidential candidates subjected to questions of email management and communication. But for DLT Solutions, the issue is not as cumbersome as it seems. The solution lies squarely in the power of a new and innovative cloud archiving service: Veritas Enterprise Vault for Amazon Web Services (Veritas EV for AWS).

GovLoop sat down with Greg Agana, a Senior Engineer and Technologist at DLT Solutions, to learn about the important features this cloud solution provides for email management within government.

Agana described the traditional process of searching and archiving emails as bulky and time-consuming. In response to records management requirements, eDiscovery, FOIA requests, and congressional inquiries, agencies are forced to filter and search manually, an endeavor that proves to take up more man hours than necessary. Given that email is at the heart of all agencies, there needed to be a solution for the unstructured data agencies created on a daily basis.

"Having to do long-type searches through email is inefficient, and there is no absolute guarantee of finding the required emails," he said. As a result, agency responses to inquiries and requests from outside entities are untimely and cumbersome. Yet there is a light at the end of an inefficient tunnel, thanks to the innovative Veritas EV for AWS, a cloud service that stores, manages and easily discovers and retrieves unstructured data.

Released recently, the Veritas EV for AWS offers an alternative to difficult searches. "It doesn't matter whether email is deleted or not, using the Vault means you are able to find necessary emails. That way, agencies can use this solution when working with multiple content sources - like email - if they're storing on the cloud. The guidelines can be utilized to reduce burdens and respond to congressional inquiries based on underlying technology, so agencies can produce reports and requests accordingly," Agana explained.

Considering the number of agency inquiries that have taken place in recent years, this tool has great ramifications in terms of streamlining a task that is usually quite the headache. It's a system that stands apart from the rest, providing unparalleled cloud security. Built on a scalable FedRAMP-compliant Infrastructure-as-a-Service cloud, the Veritas EV for AWS satisfies security needs for agency offices. It leverages AWS infrastructure, so "agencies don't have to purchase traditional servers. We can set up the infrastructure in a matter of minutes, rather than the old way, which took weeks or months to set up."

The Veritas EV for AWS allows customers to reduplicate information at the source to reduce operational costs, manage organization-wide retention and information governance policies, and control the costs of compliance and litigation support.

The cloud service solution is best characterized as a turnkey solution for a diverse set of agencies. "There are different requirements for different agencies, so we offer customization to ensure that we reach the necessary needs," Agana said about Veritas EV for AWS. "The cloud system is ready to go at any time, but it can always be adapted to an agency's workflow. The system can be utilized for defense agencies and all of government, not just civilian entities. What sets us apart is our best-of-class 24x7x365 U.S.-citizen, U.S.-soil, ITAR compliant Service Center for those in government."

Veritas EV for AWS offers support for Microsoft Exchange, Office 365, Google Gmail, and unstructured data from Sharepoint or regular file data. It starts from the Amazon Web Services infrastructure, which was deemed secure enough to host the Department of Defense's public data and some private, unclassified information. With so much capacity for a diverse set of agencies, the Veritas EV for AWS is set to redefine how agencies search and archive their data.

Released less than a year ago, the feedback has already been overwhelmingly positive, with clients within DOD, civilian and higher education spaces raving about overall speed and flexibility.

"We bring a melding of optimal infrastructures within cloud spaces and technologies from the Symantec and archiving space," Agana said, "It's a combination that results in a superior supported enterprise solution."

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 200,000 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 info@govloop.com

1152 15th St NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop

ACKNOWLEDGMENTS

Thank you to Acquia, Alliance IT, Amazon, BMC, DLT Solutions, Metalogix and ViON for their support of this valuable resource for public-sector professionals.

Authors:

Nicole Blake Johnson, Technology Writer

Designers:

Jeff Ribeira, Creative Manager
Tommy Bowen, Graphic Designer
Kaitlyn Baker, Design Fellow
Martin Nera, Design Fellow

Photo Credit:

All images in this resource are licensed by Getty Images or Creative Commons attribution licensing:

Links

1152 15th Street NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop