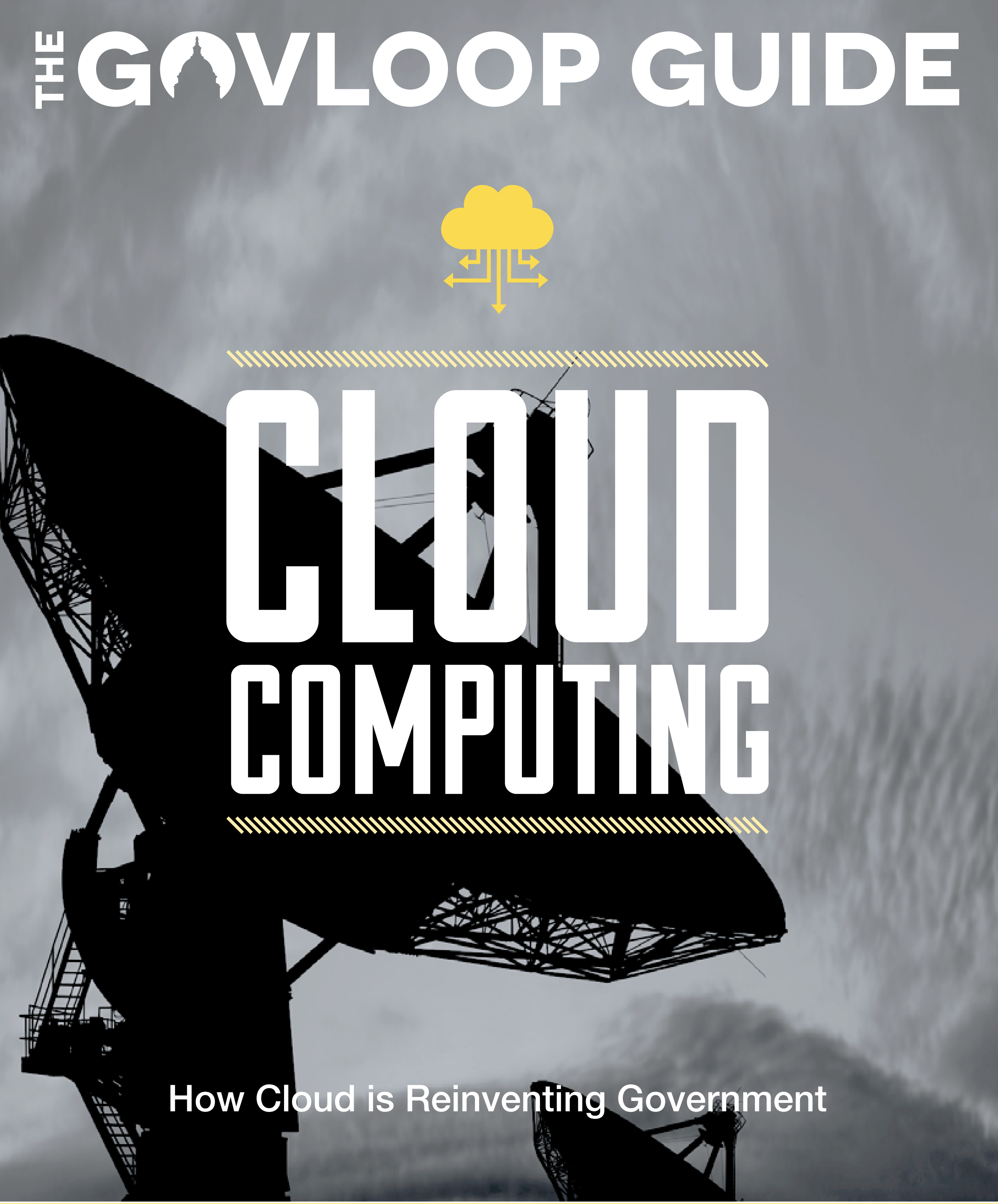


THE GOVLOOP GUIDE

CLOUD COMPUTING

How Cloud is Reinventing Government

INNOVATIONS THAT MATTER

> “WE USE CLOUD FOR EVERYTHING: IT IS NOW PART OF OUR DNA”

Tom Soderstrom, chief technology officer, NASA Jet Propulsion Laboratory

EXECUTIVE SUMMARY

This report, “How Cloud is Reinventing Government,” is your first step to understanding how cloud computing can transform your agency. Across government, agencies are building cloud infrastructures that efficiently and effectively deliver services to citizens and transform the business of government.

Part of our “Innovations That Matter” series, which explores how organizations are maximizing the latest technologies and solutions to transform their organizations, this report will teach you how to identify, customize and build your business case for cloud solutions.

GovLoop believes that cloud computing has fundamentally changed the way that government does business. It has revolutionized employees’ ability to access data, software, computing power and collaboration strategies, disrupting the traditional notions of information technology. But with these transformations comes a challenge for the public sector: How can you fully capitalize on the cloud and ensure security to advance your agency’s mission?

Our in-depth look at cloud aims to demystify this technology and help answer that question through cloud case studies , an explanation of a cloud brokerage program, strategies to securely deploy cloud and interviews with leading experts on cloud computing. This report will help you understand how to capitalize on the cloud, accelerate adoption and promote innovation at your agency.

In our research, we’ve also identified many benefits of cloud technology. Although not an exhaustive list, the items below show how powerful cloud can be in overcoming government’s toughest obstacles. Cloud can:

1. Facilitate data sharing across agencies and with the public.
2. Create a shared pool of computing resources.
3. Provide on-demand access to computing power, storage and software based on end user needs.
4. Promote green technology initiatives.
5. Improve the efficiency of government services.
6. Allow trends such as bring-your-own-device (BYOD) and telework to be broadly adopted.
7. Enable big data, mobile, geographic information systems (GIS) and related technology programs.
8. Improve the efficiency and productivity of government employees.

These benefits are just the tip of the iceberg of what cloud can do for your agency. But it all starts with identifying a clear organizational problem and then mapping to the right kind of cloud offering. By obtaining foundational knowledge and using it to inform your purchasing decisions, you’ll set your agency on the right course toward cloud adoption.

We can’t stress it enough: Cloud is a game changer and enabling emerging technology.

IS YOUR AGENCY READY?

CONTENTS

EXECUTIVE SUMMARY 1

CLOUD 101: UNDERSTANDING THE BASICS 3

FOUR REASONS AGENCIES ARE ADOPTING THE CLOUD 7

CASE STUDIES ON THE CLOUD: LESSONS LEARNED FROM GOVERNMENT'S CLOUD COMPUTING PIONEERS 9

Case Study from NASA's Jet Propolsion Laboratory

Lessons Learned from the State of Texas

Lessons Learned from the State of Illinois

Cloud Security Resources from the National Institue of Standards and Technology

ASSURING GOVERNMENTS CLOUD COMPILANCE AND SECURITY NEEDS 13

CHANGING GOVERNMENT'S PERCEPTION ON CLOUD COMPUTING 17

RE-THINKING HOW YOUR ORGANIZATION DELIVERS SERVICES 21

YOUR BEST PRACTICES FOR CLOUD ADOPTION 23

RE-IMAGINING CLOUD WITH OPEN SOURCE 27

YOUR CLOUD COMPUTING CHEAT SHEET 29

LEVERAGING CLOUD ADOPTION IN YOUR AGENCY 31

ACKNOWLEDGEMENTS 32

About GovLoop

Sponsor Acknowledgements

CLOUD 101

UNDERSTANDING THE BASICS

LESSON 1: 4 ESSENTIAL ELEMENTS OF CLOUD COMPUTING

Although the cloud has essentially transformed the business of government, our research finds there is still a significant need to educate the government workforce on the basics of cloud computing. To accelerate cloud adoption, government employees – including those who work outside traditional IT jobs – must understand what cloud is and the service and deployment models associated with it. This foundational knowledge will help officials learn how their agency can leverage the technology and capitalize on a tool that is now essential to meeting the complex demands of the public sector.

GovLoop defines cloud computing as an IT delivery model that enables on-demand access to resources, whether they are servers, computing power, applications, data or software, which can then be quickly acquired by employees using laptops, desktops or smart phones.

Some similar themes exist across the various service and deployment models of cloud. Our research identified four essential elements of cloud computing:

1. Automated and On-Demand:

Government employees may need to share large files and have additional storage. For instance, a scientist may be looking to share petabytes of weather data with a colleague across the country. Leveraging the cloud, that scientist can automatically access to the needed storage or software temporarily to transfer and process the data. When the transfer is complete, the additional processing, computing and storage capabilities can automatically return to appropriate levels.

2. Device-Agnostic:

Depending on the type of service required, the cloud is device-agnostic. Cloud can be designed to deliver resources to workstations, laptops and mobile devices. This ultimately will help facilitate the ability to work anywhere, anytime. For governments, this provides the ability to react to crises more effectively, share resources more efficiently and set up mechanisms to create resilient institutions.

3. Shared Resources:

In many cases, services are provided to many stakeholders via the cloud. Services may include computing power, data storage or bandwidth, and you may not know where the resources are physically located. For government, this is important to consider, because if data is moved between data centers to facilitate demand, you can have a sense of what data center, state or even country the information resides in. This is vital because different states and countries may have different laws pertaining to accessing and extracting data and to liabilities in the event of a data breach.

4. Scalability:

With cloud, storage, software or infrastructure can be provisioned nearly instantly to meet consumer need. In some cases, these services can be completely automated, so as demand changes, the services adjust accordingly. Such automation can help dictate and manage costs, enhance efficiencies and provide new ways to deliver services.

These four elements create the foundation to understand the cloud. Our next lesson explores how your agency can leverage the cloud.

LESSON 2: HOW YOU CAN USE THE CLOUD

Today, cloud has already made deep in-roads in government, and it's helping to re-imagine the way that government delivers services. Affecting everything from agile infrastructure to e-mail, it's clear that the cloud is having a transformative effect on the public sector.

And we're not the only ones making that assessment. "Cloud computing, [one of] the hottest trends in the IT armory, leverages leading-edge technologies to meet the information processing needs," said Michaela Iorga, senior technical security lead for cloud computing at the National Institute of Standards and Technology. "It offers a unique and complementary set of properties such as elasticity, resiliency, rapid provisioning and multi-tenancy that support cost savings both in terms of capital expenses and operational expenses."

But for government agencies, the benefits of the cloud go beyond cost savings. There's also the cloud's ability to deliver more agility and provide new efficiencies to business operations.

In the 2011 "Federal Cloud Computing Strategy"' document, then-federal government chief information officer Vivek Kundra predicted, paraphrasing Sir Arthur Eddington, the physicist who confirmed Einstein's "Theory of General Relativity," that "cloud computing will not just be more innovative than we imagine; it will be more innovative than we can imagine."

Countless stories about innovation powered by the cloud are proving Kundra's prediction right. Evidence supporting him comes from our survey of 230 public-sector employees who provided insights on how they have adopted the cloud. Their answers show the diversity of cloud applications and the many opportunities the cloud presents to transform government:

1. "Increased data sharing and storage, at reduced costs."

2. "For cloud-based e-mail, file sharing and archiving of documents."

3. "Our information technology service desk, case management system and to mointor an employee incentive program use cloud technology."

4. "Several offices use cloud services, when both government and public staff need to collaborate."

5. "To connect to programs that are on state servers, sharing data files and tracking program effectiviness."

6. "We use cloud to store information and develop dashboards."

7. "Cloud is used to store large data files that are sent from outside resources."

8. "It's essential for us to conduct assessments, valuation and create maps with GIS software."

9. "To promote telework and facilitate web meetings, document sharing and asynchronous communications."

10. "Cloud allows us to access a shared pool of tools and infrastructure."

These 10 examples are only the beginning of what you can do with the cloud. Later in this report we provide several case studies from government. But to truly make the most of cloud, understand what the technology archeticture looks like. Our third lesson will give you insights on the various service models.

LESSON 3: CLOUD SERVICE MODELS

Before looking at service models, the most important step for cloud adoption is to identify a clear problem that your organization is trying to solve. For instance, the service model will differ depending on if you need to access software across your agency, want access to more bandwidth or desire a platform to build applications. Without knowing what your agency is trying to solve, you risk uncertainty when entering the cloud marketplace and not clearly aligning your business and IT needs. We explain three cloud service models below. Each is useful for different applications of the cloud. Figure 1 explores the service models government has deployed.

Software-as-a-Service

Software-as-a-Service (SaaS) is a cloud service model in which an agency accesses software on demand from a third-party vendor. The agency does not buy the software, but is provided multiple licenses to access information. Examples of SaaS include:

- Blogging, social networking and online communications platforms.
- Online e-mail services.

Platform-as–a-Service

Platform-as-a-Service (PaaS) is a cloud delivery model in which a vendor provides an online development platform for an agency. Developers leverage the vendors' computing environments and can test, create and ultimately host new applications. Examples of PaaS include:

- Application design, development and deployment.
- Team collaboration solutions.

Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a cloud delivery model in which a vendor provides the hardware and software and a government agency can build a customized computing environment. This delivery model can provide government agencies with access to advanced computing power, storage, memory, bandwidth and software applications – all on demand. Examples of IaaS include:

- Operating systems, servers and storage capabilities.
- Networking components and software bundles.

These three service models are important – and play an important function in your cloud strategy.

The next lesson focuses on another essential element: your deployment models.

LESSON 4: CLOUD DEPLOYMENT MODELS

Once you choose a service model, the next phase is identifying the right deployment model. Generally there are four kinds of cloud deployment models: hybrid, private, public and community. Each differs in terms of who has access to information and resources.

These models are essential to understand because they dictate who and how people will access your cloud resources. Figure 2 explores the kinds of deployment models used in government, and which one officials see as the most promising.

Figure 1: [Select all that apply]

WE ARE CURRENTLY USING THE FOLLOWING SERVICE MODEL:

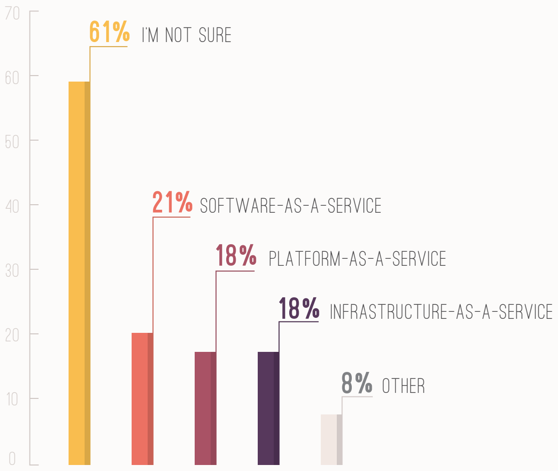
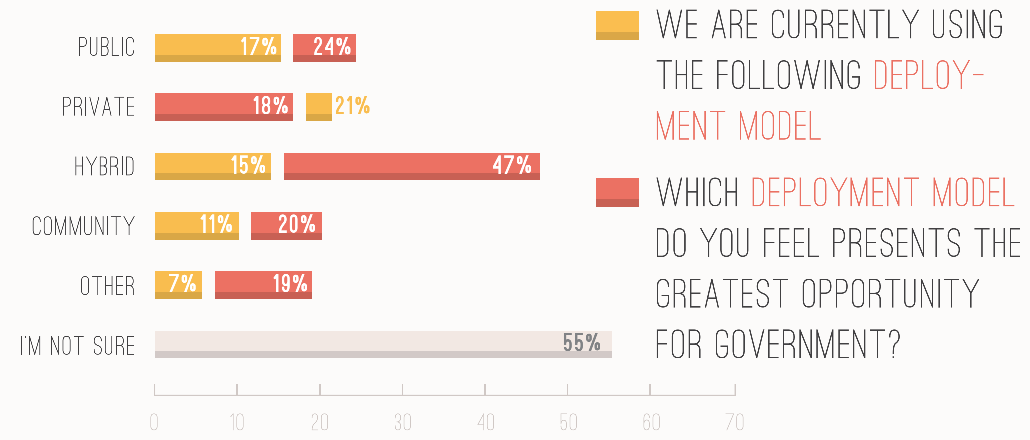


Figure 2: [Select all that apply]



The Public Cloud

A public cloud is a cloud deployment that makes information available to anyone. Our survey asked why organizations selected this type. Answers included:

- "[Public cloud] improves information sharing with lower information collection and dissemination costs."
- "Increased transparency of government and to better to serve taxpayers."
- "Helps to support open government data initatives."
- "More efficiently get information out to the general public."

The Private Cloud

A private cloud is a cloud deployment that is used exclusively for internal applications within an agency, but multiple business units may be granted access to share and manage data. Survey respondents said their agencies chose this because:

- "Private cloud is needed for Department of Defense (DoD) and sensistive information."
- "[Private cloud] has provided us easy deployment and reduced time to production for our mission."
- "For data containing personally identifiable information, it is important the data be segregated."
- "We must comply with [the Health Insurance Portability and Accountability Act] and protect sensitive information."

The Hybrid Cloud

The hybrid cloud consists of two or more deployment models. For instance, a hybrid cloud will contain both a public and private cloud and can easily segment data and transfer data between clouds as necessary. We asked our government audience why they selected a hybrid cloud. Their responses included:

- "The hybrid model allows greater daily flexibility."
- "[Hybrid cloud] allows you to dip your 'toes in the water,' while still keeping the traditional models for critical and confidential systems."
- "[Hybrid] takes the benefits of both models, public and private. There is a cost advantage from [the] public when processing non-sensitive data, and some data must stay private for confidential data for the interest of security."
- "[Hybrid] will be able to use the safety networks for a private network but will allow for adherence to transparency."

The Community Cloud

A community cloud is a model that provides access to multiple organizations that have similar interests in collaboration. You may also hear this kind of cloud referenced as a "government only" cloud model.

- "We've used [the community cloud] for grassroots initiatives and external feedback loops to local governments."
- "Leveraged the community cloud for our public participation and civic engagement campaigns, which has improved delivery of citizen centered services."
- "Community cloud has allowed us to focus information to a community of practice without sending out the information statewide."
- "Infrastructure is the last and greatest barrier to efficient provisioning of services to the public, a community cloud can help."

LESSON 5: THE FUTURE OF CLOUD

Our final lesson is a look into the crystal ball to see where the cloud might be heading. Based on our research and analysis, here are six trends that we expect to see evolve:

1. Increased case studies of hybrid and specialized clouds: Hybrid provides the flexibility of multiple models and creates more customized cloud solutions.
2. Everything-as-a-service: Nearly anything that you would use a traditional computer for – such as e-mail, web browsing or word processing – will be done via the cloud at a lower cost and with increased reliability and productivity.
3. Powering data anywhere, anytime: Data in the cloud can be managed to provide proper access, and once more standards are in place, data will become much easier to access and deploy across any device.
4. Lighter devices, with on-demand access to computing power: You will be able to seamlessly access more computing power via cloud on-demand, which will make devices lighter and reduce costs.
5. Internet of Things: Sensors and devices are now communicating with one another autonomously, and as more sensors are deployed, the cloud will play a critical role in hosting data, sharing information and serving as an on-demand outlet to pool resources.
6. Leveraging cloud brokers to manage cloud solutions: Many government agencies will be adopting multiple cloud solutions with various vendors. Cloud brokers can help manage the costs and deployment and monitor cloud programs. We explore more about brokers in our Texas case study. (See Page 14.)

These six elements are evolving very quickly, and for the NASA Jet Propulsion Laboratory (JPL), the future has already arrived. The lab provides an outstanding example of how to make the most of various cloud service and deployment models to meet mission need.

FOUR REASONS AGENCIES ARE ADOPTING THE CLOUD

An interview with Tom Ruff, vice president of public sector at Akamai Technologies.

Cloud computing is providing government agencies access to on-demand computing resources, which are needed to meet the demands of public sector service delivery.

“The cloud is also making government more proactive on the services that are provided to citizens,” added Tom Ruff, vice president of public sector at Akamai Technologies. “[Cloud] is helping agencies become not only more proactive, not only more responsive, but also more transparent in terms of how the government is helping the citizen.”

Ruff provided four additional insights into what he believes is driving cloud adoption:

1. **Government Directives:** With the OMB “cloud first” strategy, agencies are exploring various workloads that they can move to the cloud to gain cost savings and efficiencies. Also, the FedRAMP program has accelerated cloud adoption by having a clear set of standards in place to manage the adoption of cloud in the public sector.

2. **Desired Cost Savings:** In a time when government is challenged by declining budgets, agencies are looking for ways to gain cost savings. “Some of the cloud success stories show that cloud is a less expensive way of delivering the mission for agencies, so it seems to be perfect timing in the government for considering and implementing cloud solutions,” said Ruff.

3. **Secure Cloud Deployments:** Due to advancements in technology, cloud deployments can now happen safely and securely. “Government has historically looked at the cloud and seen it as a security issue. Whether it is public, private or a hybrid model, the cloud can end up being as secure, if not more secure, than many of the government implementations done on their own infrastructure, given in the cloud security soluttions that are always on and updated said Ruff.

4. **Delivering Additional Services:** The private sector now conducts many customer services over the web, and citizens today expect the same from government. The cloud offers the opportunity to expand services provided to citizens. “The government is trying to keep pace with the commercial industry and delivering new services, so whether that is leveraging social media, or streaming or mobile websites in order to have a better experience for the end user,” said Ruff.

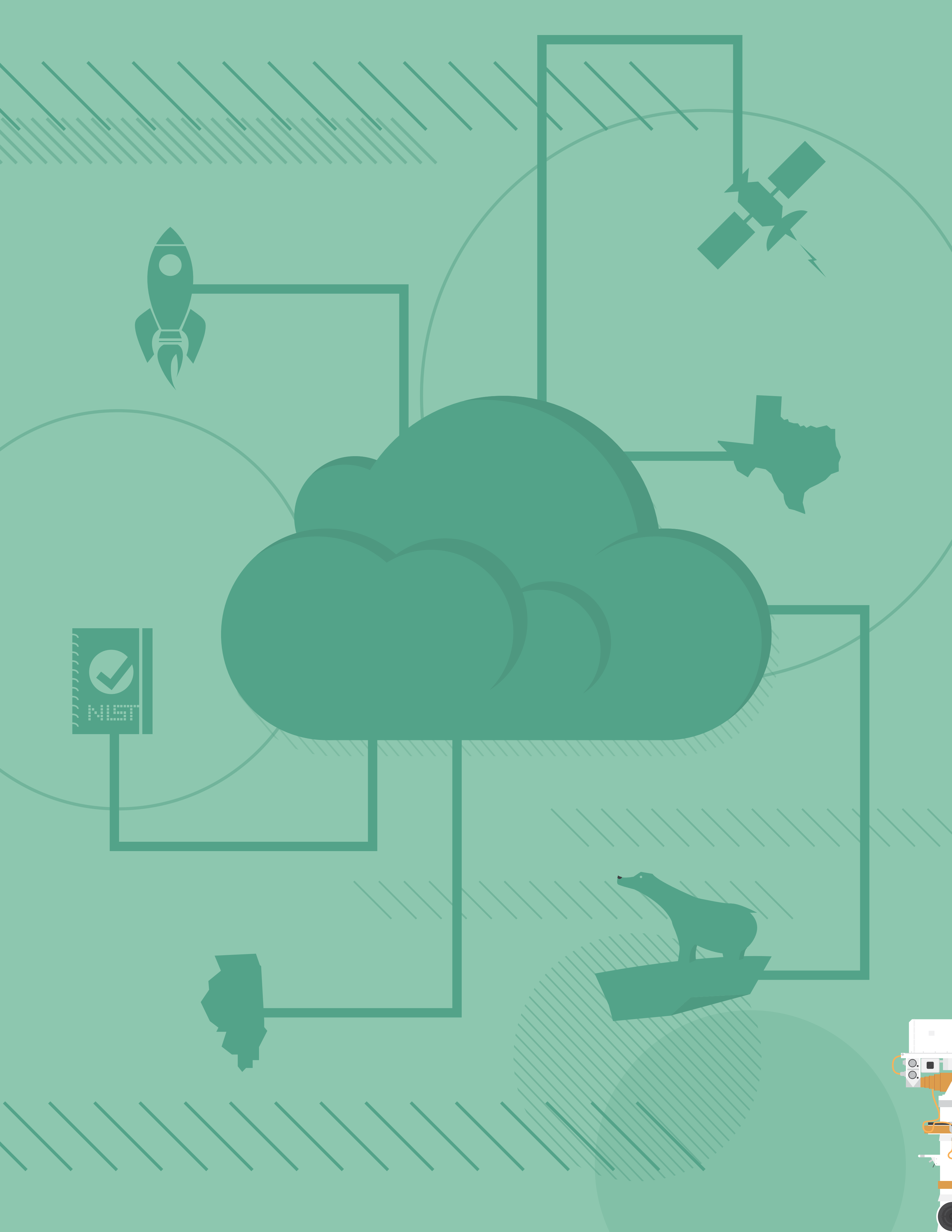
Although there are many benefits for cloud deployment, obstacles still remain for government agencies. “The number one challenge is the perception that the cloud is not secure, and that really is more of an educational gap than it is a technology gap,” said Ruff. “There is also the perception that the government loses control, where the government applications owner will feel like they will lose control or visibility, of not only the application, but also the end users and the experience.”

But with the help of Akamai, public sector agencies can have the confidence they need in a safe, secure and reliable cloud solution.

“Akamai can provide a public, private or hybrid cloud model,” said Ruff. “Akamai’s greatest example is with the World Cup. In one day, we transferred over seven petabytes of data to broadcasters – in excess of half a million users. We will see some games provide over a million users without any impact on the origin infrastructures or network of the broadcasters.” Akamai has also worked with the Department of Defense, the majority of civilian agencies, and even provided the background infrastructure to help stream events such as the State of the Union or provide cloud support with 100% availability to events such as the Census.

Akamai’s track record proves they can help government agencies meet the needs of their constituents. “What we can do for the government is what we have been doing for years,” said Ruff. “That's improving the experience, making the experience more secure and allowing the government to do its mission by allowing us to do as much work in the cloud as possible.”

Cloud computing has great promise for government agencies, and with the help of Akamai, your agency can start to be transformed or optimized by the cloud.


NIST

CASE STUDIES ON THE CLOUD:

LESSONS LEARNED FROM GOVERNMENT'S CLOUD COMPUTING PIONEERS.

MAKING THE CLOUD PART OF YOUR ORGANIZATION'S DNA

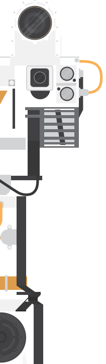
CASE STUDY FROM NASA'S JET PROPULSION LABORATORY

Nearly six years ago Tom Soderstrom, JPL's chief technology officer, set out to publish a report on what the next IT decade looked like at the agency. At the time, he envisioned a world where technology would help the public sector tackle large-scale problems and empower new ways to deliver services. Off all the technologies on the horizon, Soderstrom identified cloud computing as a potential game changer. Knowing that cloud would shape the future of how his agency operates, his team started prototyping cloud applications to gain an understanding of what the effect of cloud could be for the agency.

Today, JPL has capitalized on all the promises of the cloud and serves as a model agency for cloud deployment. "We use [cloud] for everything; it is now part of our DNA," Soderstrom said.

It's powering everything from missions to Mars to expeditions in the Arctic.

The lab's primary mission function is the development and operation of robotic planetary spacecraft. Current projects include the Mars Science Laboratory mission, which includes the Mars Curiosity rover, the Dawn mission to the dwarf planet Ceres, the Juno spacecraft heading to explore Jupiter and Kepler, a space telescope designed to analyze Earth-size planets where life and water might exist in the Milky Way galaxy.



The complexity of these missions requires support from a strong IT infrastructure. Technology is needed to give scientists, engineers and JPL employees access to the tools and resources they need.

The variety of missions means that business units will require various cloud services and deployment models. JPL shows that once a team understands the problem and mission it's trying to solve, it can map the business need to a customized cloud offering.

Soderstrom provided numerous use cases as to how JPL has leveraged the cloud to accelerate innovation and improve operations. One such example started on Nov. 26, 2011, at 10:02 a.m. EST, when Curiosity launched from Cape Canaveral Air Force Station in Florida. Powered by an Atlas V 541 rocket, Curiosity hurtled toward its next stop 127 million miles away. The rover was destined for the base of Mount Sharp, inside the Gale Crater on Mars.

Soderstrom was well aware of the historic nature of this event, and was not only on a mission with his NASA peers to land Curiosity safely on Mars, but to also share the experience with the world.

"Something like a Mars landing is our Olympics, it's our Super Bowl, it's our time when people get interested for a very short amount of time, so we can't miss it," he said.

To share the experience, Soderstrom would need to rapidly provision storage and computing power. The ultimate goal was for JPL to live stream video and photos to the web as Curiosity landed on Mars.

On Aug. 5, 2012, Curiosity reached its destination, safely arriving on Mars, ready to start exploring its new home. JPL was ready, too. It had teamed with Amazon to create the necessary infrastructure to share photos and video using a hybrid cloud.

As the landing drew closer and web visits to witness the historic event grew exponentially, JPL staff were able to access additional bandwidth on demand to accommodate increased traffic.

“We could spin up an additional 25 gigabytes per second, with a 30-second warning,” Soderstrom said. “We were able to scale up as needed until Curiosity had landed safely on Mars.”

With the cloud, “the net result was we were able to stream 150 terabytes in just a few hours, and we were able to show all the pictures that came down from Mars in real time with the world,” he said. NASA was able to conduct a public engagement initiative that it could not have done without the cloud.

For Soderstrom and JPL, the Mars landing is one of dozens of examples of how cloud computing has transformed the agency. Although deep-space missions are a major part of JPL, it also conducts significant scientific explorations here on Earth.

For instance, Soderstrom explained that periodically JPL flies over the Arctic to measure carbon dioxide levels to assess global warming. To obtain the right computing power and infrastructure needed to operate in the Arctic, NASA used IaaS and a private cloud to share data, providing computing resources to scientists in some of the world’s remotest areas.

With the Arctic mission, “we did everything in the cloud, and by doing that, we were able to save two-thirds of the computing costs for the simple reason that this particular mission flies only one or two days a month, and then planes are parked and wait for the next opportunity,” Soderstrom said. With cloud, “we could spin up all the necessary infrastructure, computing needs and storage for the mission.”

Once the project and flyovers were completed, NASA was able to shut down the cloud, and then turn everything back on when missions started again.

Cloud applications at JPL do not stop with Mars and the Arctic. As a federal agency, the lab has a strong objective to educate citizens about space exploration. To meet this mission need, JPL used a public cloud model, developing the “Moon Tours” app, which allows citizens to virtually tour the moon. The app has thousands of pictures of the moon, which are stored in Amazon’s cloud.

“You have the mobile device to visualize, to pinch and zoom, walk on the moon, explore it -- and all the heavy-duty processing that’s happening behind the scenes is happening in the cloud, including using a lot of Hadoop and slicing like Google Earth does, so that you have a good experience on the mobile device,” Soderstrom said.

JPL also connects scientists to share critical data about space and robotics projects. To meet this mission objective, it periodically hosts workshops where scientists come together to brainstorm ideas and share data from their studies. Typically, for the first half-day, they configure their laptops and systems and then copy the necessary data. At a recent workshop, however, rather than have each scientist copy his or her data to a computer, JPL used a community, or government-only, cloud, so the data was accessible there.

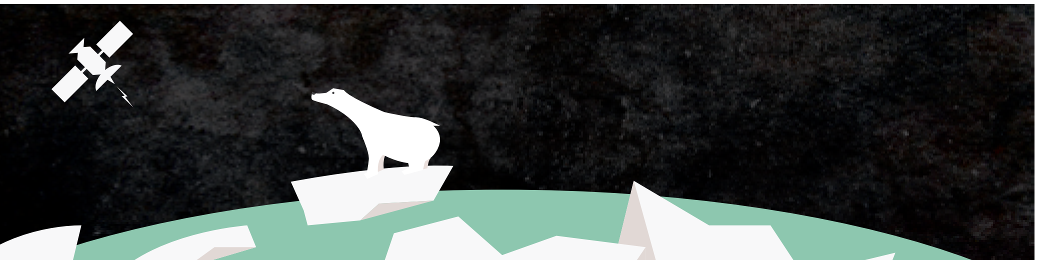
“In our two-day workshop, we were able to double the amount of work done because they didn’t have to copy the data,” Soderstrom said. “We just spun that up inside the government cloud and people could start working and sharing, and then when it was done they turned it off.”

Soderstrom said the next step will be to not only have access to data via the cloud, but also the computing power they need as well, similar to what was done during the Arctic missions.

The best is yet to come for JPL. The goal for the lab is continued disruption through technology and identifying the next cutting-edge technology. Six years ago, the cloud was at its nascent stage at JPL. Today it is essential to meeting mission needs.

“If something has social, mobile, analytics and cloud in it, it is a key disruptor,” Soderstrom said. “But there are other things that will disrupt our lives -- unless we get ahead of it like we did with the cloud. The thing that enables all of these [technologies] is the cloud. Simply put, cloud is the enabler.”

JPL not only shows the importance of mapping cloud deployment and service models to business needs, it also shows how cloud is mission-critical and capable of changing the way government meets its most complex missions – anywhere in the galaxy.



Delivering mission-critical cloud technology for over 15 years

Having delivered **secure**, accessible and massively **scalable** cloud solutions for more than 15 years to the **public sector**, GovDelivery understands the unique challenges and needs of your organization and the impact that **mission-driven** communications can have in meeting mission goals.

More than 1,000 organizations, from the *Small Business Administration* to the *Federal Emergency Management Agency* to the *U.S. Census Bureau*, already use GovDelivery's cloud-based platform to connect with over 65 million people worldwide.

How are you connecting with more people? Leverage the power of the cloud to reach more people and get your stakeholders to take action.

Learn more at *govdelivery.com/engage*.

GOVDELIVERY®

APP

ASSURING GOVERNMENTS CLOUD COMPLIANCE AND SECURITY NEEDS

An interview with C.J. Moses, general manager, Amazon Government Cloud Solutions

Faced with a unique set of challenges and requirements, public sector leaders are exploring different ways to share data and information safely and securely through the cloud.

In response to this growing market, Amazon Web Services (AWS) created AWS GovCloud (US). The AWS GovCloud allows agencies to move sensitive workloads and still achieve complex regulatory and compliance requirements for cloud deployment. AWS helps government agencies fully leverage the opportunities of the cloud, especially the ability to create a shared pool of resources and use economies of scale for cost savings.

All AWS administration, both logical and physical, is limited to US persons access within the United States. Additionally, all AWS GovCloud account holders are limited to US persons. All data is stored in the U.S. and is hosted in multiple availability zones for high durability. "What this does is allow those agencies that have U.S. persons or other controlled unclassified information requirements to be able to operate [with cloud]," said C.J. Moses, general manager, Amazon Government Cloud Solutions.

AWS helps agencies comply with the requirements of FedRAMP and U.S. International Traffic in Arms Regulations (ITAR). AWS assures the compliance and security mandates for cloud adoption that government has demanded. Additionally, the AWS GovCloud (U.S.) Region is 100% carbon-free power.

One example of an organization that is using AWS GovCloud (US) is the U.S. Centers for Disease Control and Prevention (CDC). The CDC BioSense 2.0 program provides awareness of all health-related threats and supports responses across state, local and federal government. The CDC wanted to avoid purchasing expensive hardware and software to fulfill this complicated task, so to reduce costs, and leverage hardware and software on-demand, the CDC turned to a pay-per-use model with AWS. This has also facilitated on demand usage, and assured compliance and contains world-class security practices.

Drawing from his work with public sector clients, Moses provided us with some best practices on cloud computing:

1. **Design for failure and nothing will fail:** "You have to take into account and design for failure. This is something that you could actually do in a brick and mortar traditional environment, but traditionally isn't done as much [in a cloud environment]. The idea is that you're always going to have hardware, or other types of failures happen – it's just the law of averages. If you make the software and architect the environment in such a way to accept they will fail, you can continue to work around them."

2. **Decouple your components:** "When moving to the cloud, ensure that you have the means to decouple the components of your architecture. My background includes 17 years with the U.S. federal government, and one of the things that I was regularly upset with is finding applications or architectures that were comingled in such a way that if you needed to change one thing, you had to start from scratch."

3. **Implement elasticity:** "A cloud environment gives you the ability to use additional resources in different locations, such that you're able to design for failures. So end users aren't ever affected by these failures, because you've architected your software and your implementation in such a way that you actually have the ability to work through that without them knowing."

4. **Think parallel – use multi threading:** Thinking about parallel processing helps you create repeatable processes and automate the cloud. When you must retrieve or store data, the cloud functions on parallel operations. To gain maximum efficiencies, using parallel processing is a best practice.

5. **Keep dynamic data closer to the computer and static data closer to the end-user:** This is a best practice because by doing so, you can reduce latency by keeping your computing or processing close to data.

Moses' insights provide clarity about the power of the cloud, and reveal how Amazon Web Services can help you deploy a safe and secure cloud-computing strategy.

NAVIGATING THE CLOUD: DO YOU NEED A CLOUD BROKER?

LESSONS LEARNED FROM THE STATE OF TEXAS

In 2011, officials at the Texas Department of Information Resources (DIR) realized cloud computing was essential to supporting the various missions of state agencies. Seeking to reduce costs and increase efficiencies through smart IT investment, DIR started a cloud pilot program, specifically designed to understand the contractual and operational components of cloud computing, and how to spur adoption of cloud services.

The 12-month pilot program allowed three agencies to customize a cloud solution from a variety of pre-approved cloud service providers. The resources could be procured through a central self-service web portal, and then information was collected and shared to inform future cloud implementations across government.

“During the DIR pilot, we were focused on uncovering the realities and the myths of adopting cloud services, and see how the public sector reacts to having react to a marketplace where you don’t have to go through a lengthy procurement cycle,” said Todd Kimbriel, director of e-government and IT services at DIR.

When accessing the self-service portal, agencies worked with a cloud broker to help build their customized solutions via the vendors in the pre-approved marketplace. With the broker, they had a single entity helping design, procure, provision, monitor and govern the cloud services.

“It’s the responsibility of the broker to really affect a translation between what the capabilities of the cloud provider and customer demands are,” Kimbriel said.

“[Cloud brokers] not only bridge the gap, but also provide value-added services,” he said. “In our case, the purpose of the broker is to actually be a single point of contact for whatever the cloud services are. The idea is that that cloud broker becomes the expert on how to configure and consume those cloud services, how to ensure that the service-level agreements are held. It’s almost a governance role, as their job is to govern the service delivery from cloud providers.”

The pilot program enabled DIR officials to learn more about cloud and how to structure cloud contracts. According to a report published by the pilot team, the program taught them about:

- Provider selection.
- Pricing and access security.
- Data security and credentialing.
- Provisioning time frames.
- Service levels.
- Service remedy options.
- Terms of use.
- Billing models.
- Interoperability.
- Mobility.
- Scalability.
- Capacity management.
- Provider compliance and monitoring and licensing.

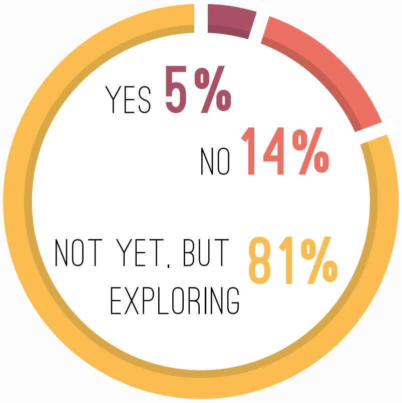


Figure 3:

DOES YOUR AGENCY USE A CLOUD BROKER?

For public-sector agencies, cloud brokers will continue to become more important. Because of cloud’s complexity, one service provider may not be able to provide all the requirements that an agency has. That’s where a cloud broker can help create a customized cloud solution.

As the Texas case study shows, cloud brokers manage the cloud adoption process and integrate everything into a single location, helping you centrally manage numerous platforms and services. Our data finds that a majority of our respondents have yet to use a cloud broker (Figure 3). Part of that might come from confusion. A standard definition of a cloud broker is hard to come by, but the basics include:

- Centrally managing multiple cloud solutions, helping to reduce costs and improving efficiency of IT solutions across an agency.
- Vetting a vendor to be sure that it meets the agency’s security and compliance standards.
- Helping with the quick provisioning of additional services.

In Texas, the pilot program has enabled more agencies to easily procure the cloud.

“[Cloud is] kind of like a Rubik’s Cube with a lot of different pressures and demands that you have to sort of figure out, like the right ballet on a high wire,” Kimbriel said. “There’s a way to do it, and it’s different for every high wire, but you have to figure it out based on the context the specific need that you’re serving.”

As cloud adoption continues to increase, the role of the broker will become more important. Agencies will not be able to look at the cloud in terms of just one solution, but rather across the entire organization. In doing so, organizations can expedite the procurement process and leverage existing cloud infrastructure.

MAKING THE BUSINESS CASE FOR CLOUD COMPUTING

LESSONS LEARNED FROM THE STATE OF ILLINOIS

The state of Illinois has taken a “cloud first” approach to computing. Mirroring related strategies at the federal level, Illinois is looking to encourage agencies to consider cloud before making new IT investments. In March, the state house passed House Bill 1040, which encourages all state agencies to consider cloud-based options when making new technology investments.

“[The bill] posture all of the agencies in the executive branch is to move to software-, platform- and infrastructure-as-a-service as the way to support future business needs. The bill helps us to make optimal use of emergent trends in technologies, and therefore, most effectively support policy and business initiatives,” said Sean Vinck, CIO for the state of Illinois.

The bill builds on an executive order from Gov. Pat Quinn. The mandate makes open data a priority and requires agencies to think open first when deploying new IT systems.

“What [the bill] is saying is that as you’re conceiving new business initiatives and making new technology investments to replace legacy systems, we want people to do their due diligence and strategic sourcing, examining the entire marketplace for options,” Vinck said.

The mandate is forcing officials at agencies in Illinois to think about the business benefits of doing things traditionally, and measuring the costs, risks and considering emerging tools.

“If you perform a calculation and look at all of the factors, you are going to find that you’re better postured leveraging emerging technology,” Vinck said. “For example, you’re better off leveraging software-as-a-service to support application development, rather than the traditional method of IT modernization.”

Even though the value proposition for cloud is there, organizations still need to learn how to make the business case for cloud adoption to gain buy-in across agencies. Vinck provided some strategies on how to make the business case to help support cloud deployment.

“First, people need to have a very healthy assessment of what their current risk profile is and what their cost structures are,” said Vinck. Making the business case for the cloud means you need to start by asking the right questions. To do so, agencies should explore:

1. What is the current level of risk? What is our risk tolerance?
2. What is the trajectory of risk? How can we manage risk?
3. What does cloud mean for our workforce?
4. What kind of SLAs do we need?
5. What kind of SLAs can we reasonably enforce?
6. What do we do at the end of the contract term?
7. How do we address the problem of vendor lock-in?
8. How will these solutions save us time and efficiency compared to traditional methods?
9. How does this transition affect our workforce?
10. Are we solving the right problem? Will this investment facilitate improved service delivery?

Although these questions are likely to be answered, there will always be inherent risks in adopting the cloud. With any new kind of IT deployment, there are always associated risks beyond the scope of what IT can control.

To mitigate the risks and challenges associated with cloud procurement, Illinois is looking to create a set of IT contracts and solicitation documents that are tailored for the cloud. This way, people can use them as a template for their own projects.

“One thing we can do is to provide a library of template solicitations and contracts and expand our efforts to continually revise a standard form service-level agreement that people can reference and consider when working with vendors,” Vinck said.

This process will not only help agencies build their business cases, but it also empowers teams closest to the challenges to identify the right cloud-based solutions. With cloud computing, it will always be the employees closest to the process and problems who will be able to govern and manage cloud best.

But across all cloud deployments, there are some standards that cannot be compromised. Government has an obligation to obtain the highest level of security, safeguard public data and be proper stewards of public resources. Within state government, various business units and agencies will need flexibility to meet their objectives.

“With the state agencies we need a baseline principle that we respect in a common way,” Vinck said. “But the business requirements with each agency may be as different as Texas, Washington and Maine, and that’s fine.”

For state governments, the path toward increased cloud adoption is helping agencies define their business and create baseline security standards, while still providing flexibility to meet business units’ mission need.

> ***“You’re never going to be able to anticipate what every possible problem is. But that’s not a sufficient argument not to make the move,” Vinck said. “You come up with reasonable and effective ways to mitigate [risks], and you move forward. But you do it gradually, and don’t put all your eggs in one basket.”***

MeriTalk IN PARTNERSHIP WITH BROCADE

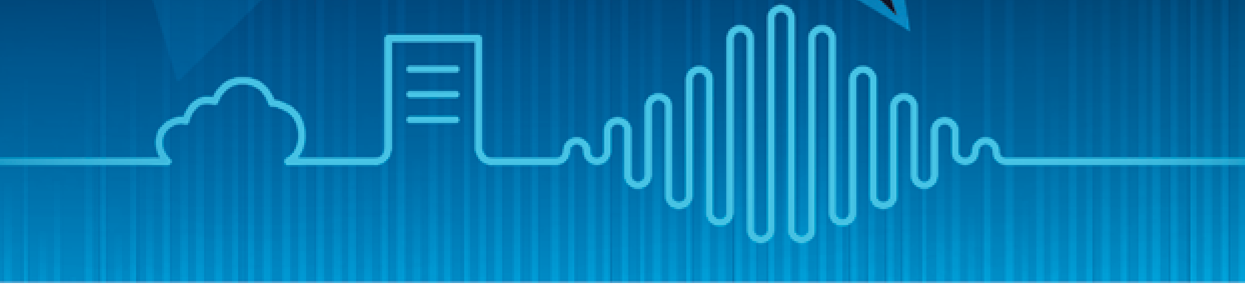
FEDERAL FORUM 2014

08.13.14

RONALD REAGAN BUILDING AND
INTERNATIONAL TRADE CENTER
WASHINGTON, D.C.

FEDERAL NETWORKS

THE NEW CONVERSATIONS



Are you ready to change the network conversation?

Don't miss out. Attend the 2014 Federal Forum to hear insights on how agencies can change the conversation and bring networks to the forefront of data center modernization.

Why attend? Sessions will allow attendees to learn how to:

- Optimize your network for data center transformation
- Shift budget money to invest in new technologies
- Take the next step on Software-Defined Networking

Attendees will take away actionable insights that will help transform the network conversation from getting the most out of the old to harnessing the new.

Event Details

Where: Ronald Reagan Building and International Trade Center Washington, D.C.

When: August 13, 2014
Registration begins at 7:00 a.m.

Program runs from 8:15 a.m. to 2:45 p.m.

There is no cost to attend.

Register Today

www.federalforum2014.com

CHANGING GOVERNMENT'S PERCEPTION ON CLOUD COMPUTING

An interview with Chip Copper, principal engineer, Brocade

Cloud computing is offering government new ways to reimagine how services are delivered to citizens and how business functions can be executed. And with the federal government's FedRAMP initiative, government agencies now have the chance to adopt state-of-the-art cloud solutions.

"This is a fundamental mind shift in the way services will be fulfilled. Application owners will now have a much greater say in choosing the vehicles that will satisfy business requirements while staying within government business and security constraints," said Chip Copper, principal engineer, Brocade, in an interview with GovLoop.

As our guide has shown, the cloud provides many different benefits that help drive innovation in government. "The cloud brings technologies that change the way IT providers do business. These technologies are now available for use by in-house IT providers. The speed, quality, and cost of services are bringing users to the cloud," said Copper. "As these technologies find their way into government data centers, those data centers will become more competitive and capable, and in several years, we may even see the current exodus out of the data center reversing itself."

Changing the government mindset will not be simple; for decades, government has built infrastructures that do not easily communicate with one other. But with the cloud, government now has an opportunity to build safe, scalable, and secure cloud solutions to improve government efficiency. Using cloud technology, government agencies can deploy solutions on-demand, and receive access to infrastructures, without having to buy expensive set-ups.

So what can government do to start changing its mindset around the cloud? Copper advised just being open to the idea of trying the cloud as a new service delivery model.

"Too many IT professionals have determined that the cloud is inappropriate for government business based on either a lack of information or on outdated assumptions," Copper explained. "The cloud service providers want government business, and have hardened and refined their services to be suitable for government use. These same providers have opened themselves up to the government for examination, and to the surprise of many government IT professionals, they have passed the test."

Government agencies are looking for vendors and professionals who can help them quickly and efficiently make the move to the cloud. That's where Brocade can help.

"Moving to the cloud should be evolutionary, not revolutionary. By complementing existing infrastructure with software defined networking-based bridges, a controlled, efficient, and secure transition to the cloud can take place," said Copper.

To prepare the way for Software-Defined Networking (SDN), Ethernet fabrics based on Brocade VCS Fabric technology help organizations create efficient data center networks that just work. Brocade fabrics provide unmatched automation, efficiency, and VM awareness compared to traditional network architectures and competitive fabric offerings.

"Brocade knows how to help organizations prepare for the cloud, and has been doing it for commercial and some government customers for a very long time," said Copper. "With information as important as that which the government has, it is critical to partner with a networking company that has this type of experience. This is not a place for experimentation, and Brocade has some of the best engineers in the world to bring world-class solutions to government agencies."

Brocade is actively engaged with partners on open industry initiatives, such as OpenDaylight and OpenStack, advancing their capabilities and providing seamless interoperability between platform layers. Additionally, Brocade is aggressively partnering with several vendor ecosystems that are delivering solutions that build upon various combinations of these platform capabilities. For example, the Network Functions Virtualization (NFV) Connection Services components of the Brocade Vyatta Platform are anchored through the Layer 3-7 capabilities of the Brocade Vyatta vRouter and Brocade vADX products, which are available today and deployed worldwide.

It's simple: the cloud has changed the way government does business and delivers services to citizens. You can help change the perception of the cloud at your agency, and use it as a tool to drive innovation.

BEING GOOD STEWARDS OF TECHNOLOGY: FIRST STEPS TO SECURING THE CLOUD

CLOUD SECURITY RESOURCES FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

According to our survey results, cloud security was one of the leading challenges respondents cited. In the following Q&A, Michaela Iorga, senior security technical lead for cloud computing, National Institute of Science and Technology (NIST), offered her expert insights on how to remain safe and secure with the cloud.

What security challenges do agencies face when adopting cloud?

Iorga: In 2010, the federal CIO introduced the "25 Point Implementation Plan to Reform Federal Information Technology Management," highlighting the strategic shift to a "cloud first" policy. It tasked NIST and other agencies with specific activities aimed at accelerating the adoption of cloud computing.

Acknowledging that key to achieving cloud adoption is addressing the security and privacy concerns that federal agencies have about migrating their services to a cloud ecosystem, NIST researched and documented agencies' top security and privacy concerns and challenges in "Challenging Security Requirements for the US Government Cloud Computing Adoption," a white paper available here. It is important to note that this white paper is not comprehensive. It offers a snapshot of security challenges perceived as impediments in the early stage of government's cloud adoption. NIST is a non-regulatory agency and therefore does not monitor any agency's challenges or performance regarding cloud adoption. It used the results of the research only to better plan its activities that fall under agency's mission.

Challenges that surfaced inNIST's research and the "Intersection of Cloud and Mobility Forum and Workshop" in March involve authorization, authentication, privacy, confidentiality, and non-repudiation processes and mechanisms. Also, because cloud computing offers a new, elastic, data-centric paradigm that moves away from the traditional perimeter-based approach toward a layered model with split management of functional layers among cloud actors, ensuring the proper isolation of data in this multitenant environment requires special attention and can be challenging. Engineering governance and monitoring solutions that address the security and privacy requirements need to be embedded in all functional layers to confer good evidence of a complete solution that covers the entire cloud ecosystem: hardware, software, people and processes.

What are some best practices for cloud security?

Iorga: Cloud computing faces many of the same threats as classical IT systems, and although the cloud computing industry is experiencing tremendous growth due to its benefits, we also have seen an increase in criminal activities in the cloud.

The presence of massive amounts of valuable data from multiple entities in a single cloud infrastructure creates an extra-attractive target, worth the effort invested in maliciously accessing, stealing or compromising it. For government agencies, securing the IT systems to meet Federal Information Security Management Act of 2002 requirements is not a new task. We've been implementing secure IT systems for long enough to know what we want to achieve.

NIST's mission is to support agencies' migration to the cloud through standards, measurements and technologies. In scope with our mission, NIST posted for public comments in 2013 the "NIST Special Publication 500-299: Cloud Computing Security Reference Architecture," that provides a security overlay to "NIST SP 500-292: Cloud Computing Reference Architecture," and a methodology for architecting a secure cloud ecosystem. We are currently in the last phase of finalizing this document. "SP 500-299" was developed with public support as collaborative work done by the NIST Cloud Computing Security Working Group, therefore introducing a publicly vetted cloud framework.

In a building block approach, NIST will continue fulfilling its mission in terms of providing security guidance to government agencies by working on a "Cloud-adapted Risk Management Framework" document derived from the "NIST SP 800-37" and a "Cloud Overlay" document based on the "NIST SP 800-53 R4" security controls. Furthermore, to address agencies' security concerns, NIST is planning on working on security SLAs as part of the current NIST effort of standardizing SLAs and SLA metrics.

How can NIST help agencies remain secure when adopting the cloud?

Iorga: Since government agencies retain the responsibility of meeting the mandates of FISMA, depending upon the type of data, services or applications migrated to the cloud, agencies must ensure that their SLAs legally bind the cloud provider, broker or carrier to implement all "NIST SP 800-53" security controls they deemed appropriate and applicable.

NIST is not a regulatory organization, but FISMA and Office of Management and Budget policy require cloud providers that handle federal information or that are operating information systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies. Security and privacy requirements for cloud providers, brokers and carriers, including the security and privacy controls for information systems processing, storing or transmitting federal information, need to be expressed in appropriate contracts or other formal agreements using the "Risk Management Framework" and associated NIST security standards and guidelines. However, as indicated in the "NIST SP 800-37" document, the security authorization of the service remains an inherent federal responsibility linked to the management of risk related to the use of cloud services.

How can an agency get started with cloud computing?

Iorga: The main key element is agencies' understanding of the roles and responsibilities of all cloud actors involved in the orchestration of the cloud ecosystem they are procuring -- agencies as cloud consumers and cloud providers, brokers and carriers as vendors of different services or capabilities.

It is also important for the agencies to leverage the Federal Risk and Authorization Management Program assessment and authorization process while diligently identifying the controls that require tailoring to meet their IT systems needs. Pushing their security requirements through SLAs to the cloud providers and broker is key to preserving the post-migration security posture of their system. "NIST SP 500-299" introduces a methodology for orchestrating a secure cloud ecosystem. Complementing specifications are currently in the pipeline.

Iorga's insights provide you with an initial framework on how to safely and securely deploy the cloud. For more information on NIST and best practices, please view its resources on cloud.

> "THE MAIN KEY ELEMENT IS AGENCIES' UNDERSTANDING OF THE ROLES AND RESPONSIBILITIES OF ALL CLOUD ACTORS INVOLVED IN THE ORCHESTRATION OF THE CLOUD ECOSYSTEM THEY ARE PROCURING -- AGENCIES AS CLOUD CONSUMERS AND CLOUD PROVIDERS, BROKERS AND CARRIERS AS VENDORS OF DIFFERENT SERVICES OR CAPABILITIES."
>
> *- Michaela Iorga, senior security technical lead for cloud computing, NIST*

We see a cloud where your data lives without limits.

Choose the right cloud solution that works for you.

LEARN MORE

UnboundCloud™
The new vision of cloud
data management

NetApp®

RE-THINKING HOW YOUR ORGANIZATION DELIVERS SERVICES

An interview with Kirk Kern, chief technology officer, NetApp U.S. Public Sector

Faced with declining budgets and revenues, Chief Technology Officers, Chief Information Officers and information technology system managers are being forced to re-evaluate IT systems and discover new ways to cut costs. As a result, many government agencies are turning to cloud computing as a means to re-think the way their organization delivers technology services.

"Government is turning to the cloud in an effort to reduce cost and improve efficiency," said Kirk Kern, chief technology officer, NetApp U.S. Public Sector, in an interview with GovLoop. "They are starting to look at new ways to bring systems online to improve IT service delivery by using private clouds within their data centers. In other cases they're turning to public clouds, where the data and the services can be generated entirely over the network and then delivered from an off-premise resource to their agency."

Added Kern, "In many cases, we're also seeing hybrid approaches where the agencies are consuming elastic and on demand public cloud services, while still retaining some on premise compute, or data storage capabilities."

Although many agencies have made the move to the cloud, some are still dealing with many challenges in cloud adoption. One main hurdle can be identifying the right kinds of workloads to move to the cloud, and making a decision on what will help a government agency with their mission.

"The services or the workloads that the government is attempting to migrate to the cloud, or to leverage cloud resources, are no longer constrained [by application]. Virtually all services are being evaluated for migration to the cloud," said Kern.

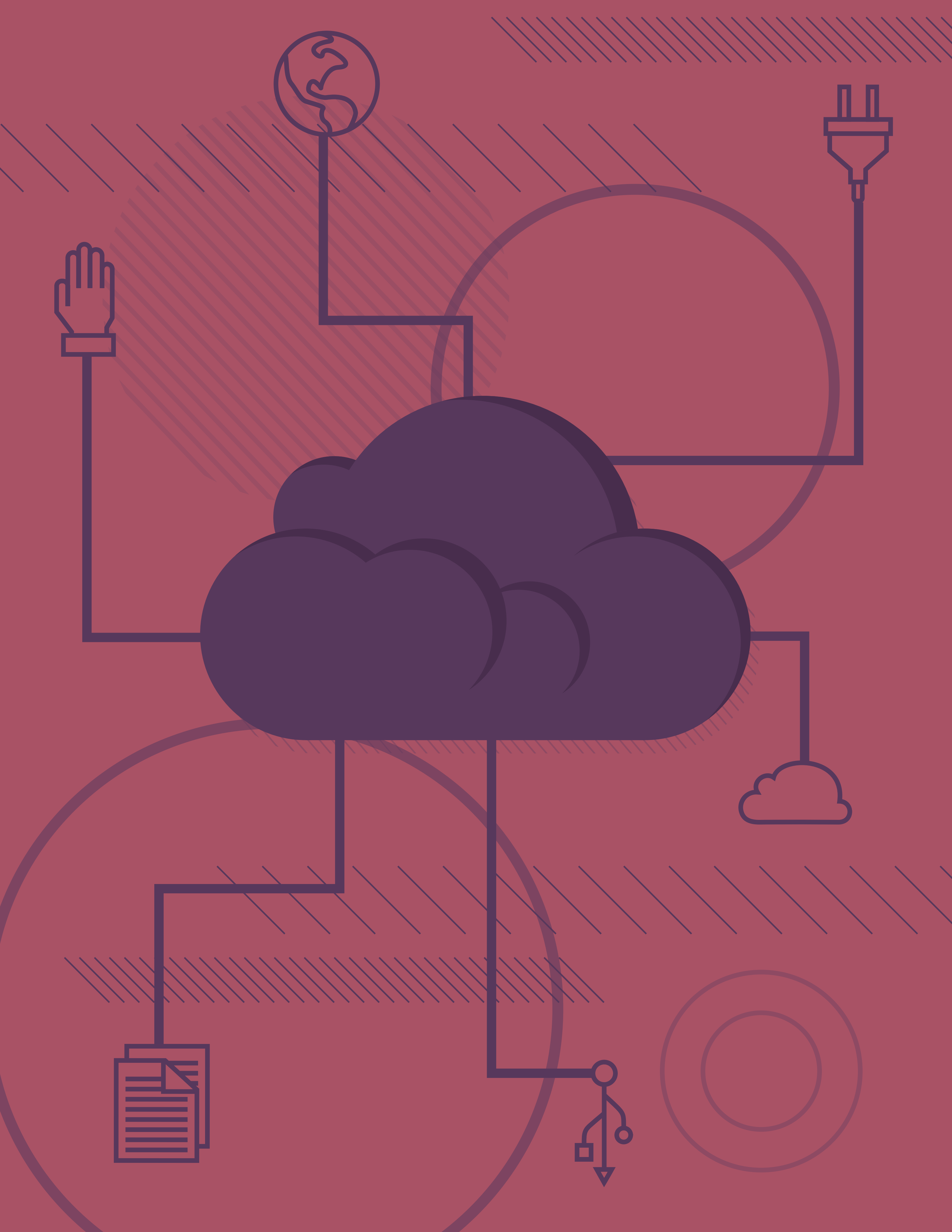
These services include everything from accounting and finance, payroll, personnel databases, communication systems or any service that is part of the mission function of an agency. Ultimately, this move to cloud is occurring because of the pressures on government administrators to identify cost savings. As more services become virtualized, it is important to remember that although the service is in the cloud, agencies must still pay close attention to data management.

"As computer services are becoming stateless, the data management and the ability to move information across clouds [is important]," Kern explained. "IT professionals still have to come up with techniques in order to accomplish [moving data]. Even with today's networks, in order to move a petabyte from one data center to another, many customers find that it's cost prohibitive, and that they can't afford to move a petabyte in a timely fashion, or in some cases, these datasets are just so large you cannot move them."

One of the ways to avoid this obstacle is to be sure that your organization has selected the right workload for cloud migration and right size for your cloud solution. "A lot of times agencies need to take a step back and start with their organization or agency's goals or mission," Kern said. "From there you can define the services required to support those goals. That has more value than just picking an individual service, because it's actually going to help the agency accomplish its task."

For government agencies, Avnet Government Solutions is uniquely positioned to help agencies adopt the cloud. "For private and hybrid clouds, we provide the infrastructure solutions that enable cloud in agency data centers, we provide pre-integration of infrastructure services, we provide professional services to design and develop an agencies CloudOS approach, the automation, service catalog integration with other clouds and the business alignment required for successful cloud implementation," said Darren House, director of solutions management, Avnet Government Solutions. "Whether an agency needs private, hybrid, public or any combination, Avnet Government Solutions has the technology, services and financial solutions that will help agencies adopt cloud."

To continue to expedite adoption of the cloud in the public sector, agencies must continue to align cloud to mission need, and then partner with a vendor who can provide the security, flexibility and scalability required to meet the needs of the public sector.



YOUR BEST PRACTICES FOR CLOUD ADOPTION

10 BEST PRACTICES YOU NEED TO KNOW TO START YOUR JOURNEY TO ADOPTING THE CLOUD

1. MATCH PROBLEMS TO IT SOLUTIONS.

For cloud computing adoption to truly accelerate at your agency, it is essential to identify a clear problem that you are trying to solve and the right cloud deployment and service model for it. “The challenge is to match up the problem you’re trying to solve with a cloud offering,” Soderstrom said.

2. NAVIGATE CULTURAL BARRIERS.

To navigate cultural barriers, you will need to build support from various stakeholders. This means being sure that you are collaborating across teams and have all the right voices at the table. “You need a champion,” Soderstrom said. “So in our case, the CIO, Jim Renaldi, was very forward-looking. That was a big deal, because it gave direction for everybody. And that it’s OK to explore [new technologies], and you’re not going under the radar and have to worry about being detected.”

3. ENGAGE LEGAL TEAMS TO UNDERSTAND THE EVOLVING ENVIRONMENT.

When starting any cloud initiative, you should engage legal teams upfront to understand what is appropriate cloud usage and what is not. “Legal needs to be an enabler, not a disabler, saying, ‘Here’s how we can do [cloud] appropriately,’” Soderstrom said. By engaging the legal team early, you can work collaboratively to navigate obstacles and fight off any challenges early in the process.

4. DEFINE DATA OWNERSHIP.

When developing your SLA, you must be able to clearly articulate the right kind of data ownership policies. “Confidentiality of information, control over information, what happens if the Interent goes down, who will control the data center operating the cloud -- these all must be defined upfront,” said a survey participant.

5. COLLABORATE AND SPEAK THE RIGHT LANGUAGE.

"It's important to align the capabilities of the providers to the needs of the customers, and get them to talk in the same language," Kimbriel said. When working on cloud deployments, teams must be able to talk both the IT and business languages to drive the highest value and decide on the right cloud offering.

6. START SMALL AND PILOT TEST.

Our research also showed that it is essential to test cloud and start small. "A recommendation is to do lots of testing and use in non-risk areas to learn about the 'new' world and next step in technology," a survey participant said. "Start with the easiest, least-controversial and most useful stuff first. Early victories build momentum, and you can develop your processes in a safer environment," another said.

When considering how to test cloud, Soderstrom also advises two points

- "Test the cloud on something real -- a problem you need to solve. But something that is not so big and daunting that it will fall under its own weight because you're just starting out, you're trying something new," he said.
- "Do not test on legacy pieces. If you take your legacy app and you put it into a new environment, it's bound to not perform as well as it does in the existing environment. So try something new. Try something that is in the IT queue, because the primary benefit of the cloud is speed to market," Soderstrom said.

7. PROACTIVELY ADDRESS SECURITY CONCERNS.

Managing security is an important step toward cloud adoption. "Consider the freeway. Is the freeway secure? Is the cloud secure? The freeway is very secure if you're driving in a big tank. It's not secure if you're blindfolded on a bicycle. It's what you do on the cloud that matters. It's how you drive on the freeway or how you use the cloud," he said.

8. INCREASE EDUCATIONAL OPPORTUNITIES.

Another best practice and need is to educate the workforce. Our survey asked: "Does your agency provide training on securely using the cloud?" Eighty percent of respondents said no. Agencies must train employees on how the cloud is being used and appropriate ways to share information through it.

9. FORM A SMALL TEAM THAT MEETS FREQUENTLY.

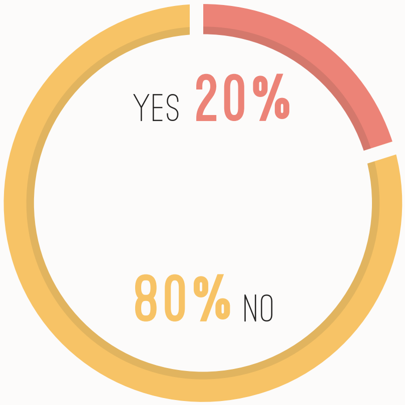
In all our case studies, one of the common themes was that a small team of stakeholders was created to navigate cloud procurement. "A recommendation is to form a small team that meets very frequently and forms personal relationships so that they can cut through and identify what looks difficult and talk about it quickly and directly. That's what we did at JPL and it was very successful. It took a while, but it was very successful. It'll last through future innovations," Soderstrom said.

10. CLASSIFY YOUR DATA.

Remaining secure in the cloud starts by understanding your data, what data is highly sensitive and who has access to information. "One of the fundamental elements of building a security plan is to have a data classification policy. And that determines which of your data needs what level of security wrapped around it. If you understand your data, and you understand what security that data requires, then from that you can make the appropriate decision about public or private cloud," Kimbriel said.

Figure 4:

DOES YOUR AGENCY PROVIDE TRAINING ON SECURELY USING THE CLOUD?



redhat.

Close the gap between what your agency needs and what the IT organization can provide.

IT budgets are **SHRINKING**[1]

Demands on IT are **INCREASING**

70% of IT budget is spent keeping lights on[1]

Organizations are turning to cloud to close the IT delivery gap.

More than **90%** of **Fortune 500** companies use Red Hat products and solutions.[2]

80% of top public clouds are built on Linux® and open source.[3]

#1 corporate contributor to OpenStack® for the last 3 releases.[4]

With Red Hat, government agencies protect citizens and serve the warfighter by providing greater agility and flexibility, and preparing for the future.

RED HAT'S AWARD-WINNING CLOUD PORTFOLIO

OPENSTACK FOR IaaS

OPENSHIFT FOR PaaS

RED HAT CLOUDFORMS FOR CLOUD MANAGEMENT

RED HAT JBOSS TECHNOLOGIES FOR NEXT-GENERATION CLOUD APPS

AWARDS

RED HAT CLOUD INFRASTRUCTURE
IDG Techworld Awards 2013: SaaS product of the year

RED HAT CLOUDFORMS
2014 Virtualization Review Editor's Choice award, best virtualization management

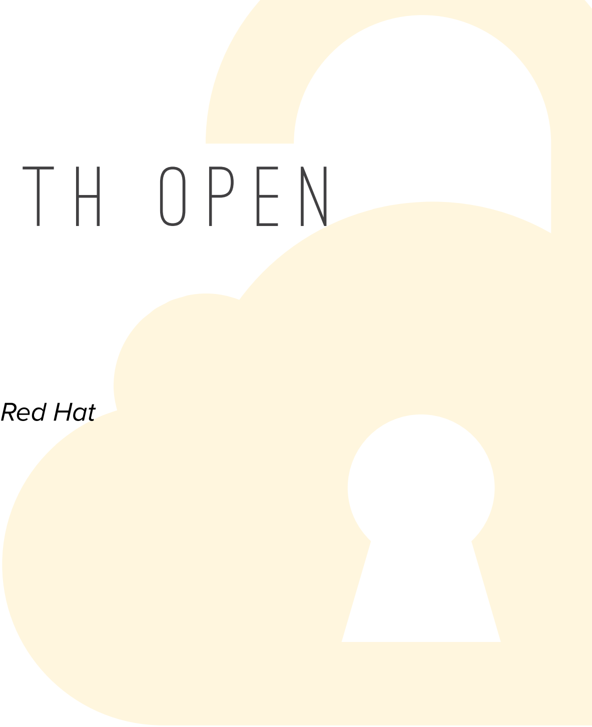
OPENSHIFT BY RED HAT
Asia Cloud Awards 2013: Best PaaS

Gartner Magic Quadrant

2014 American Technology Award for Cloud Computing

[1] United States Government Accountability Office, "Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments," October 2012 GAO-13-87. *Weighted average IT budgets change – weighted by 2013 IT budget size. [2] Red Hat client data, 2013. [3] "Linux Adoption Trends 2012: A Survey of Enterprise End Users," Linux Foundation. [4] Source: OpenStack Grizzly release contributions | OpenStack Havana release contributions.

RE-IMAGINING CLOUD WITH OPEN SOURCE



An interview with Gunnar Hellekson, chief technology strategist, public sector, Red Hat

Government has used open source solutions in a variety of different ways – for everything from powering government websites to running communications platforms. For government to truly re-invent themselves with smart technology investments like cloud, open source plays an essential role.

“Open source makes cloud computing possible,” said Gunnar Hellekson, chief technology strategist, public sector, Red Hat, in an interview with GovLoop. “There are two reasons for this: cost and ubiquity.”

The benefits of open source include reduced costs and improved efficiencies. When leveraged with a cloud solution, agencies gain the benefits of both. This combination creates a powerful IT infrastructure that is flexible, scalable and resilient enough to meet the complex demands of public sector IT delivery. It also provides access to an open source community who can collectively work to address challenges and share best practices amongst each other.

“Open source projects provide a place for cloud providers and users to build consensus on the best solutions and make those best practices immediately available to everyone,” said Hellekson. “Companies like Amazon, Netflix, Yahoo, and Google regularly release new open source projects so they can work with the larger open source community on these problems.”

The benefits of an open cloud model extend to it being a secure IT solution. As the market has matured, and programs like FedRAMP have continued to develop, agency leaders are increasingly gaining the confidence they need to know that cloud is a safe and secure solution. For government agencies using cloud, security will always be a concern, but its use does not present the same kind of roadblocks as it did in the past.

“The greatest threat isn't security in the traditional sense,” said Hellekson. “It's the unprecedented consolidation of government computing to a relatively small number of cloud providers. With that in mind, it's more important than ever that agencies have the tools and policy they need to ensure that their exit from a cloud provider is as easy as the entry. If you can't easily quit your cloud provider, you're vulnerable to price hikes, bad service, and the other hallmarks of lock-in.”

Hellekson shared one example from a client who has deployed Red Hat’s platform-as-a-service solution, OpenShift. “This bureau is very federated, and wanted to provide its developers with a single, standardized platform to build applications on. The trick is they had to make that platform attractive enough that all the offices and programs underneath them would be willing to migrate,” said Hellekson. “OpenShift was perfect, because it gave them a platform they could standardize on, and still operate it wherever they need: in a public cloud, in the central data center, or in one of the offices. The standardization lowers their operating expenses, and the developers are much more effective because they don't have to worry about operational concerns.”

Red Hat is helping government adopt safe and reliable cloud solutions by leveraging an open source platform. “We're working with one agency who was pretty happy with their VMware infrastructure, but didn't care for how much money it cost. They wanted a lower-cost alternative, and found it in our Red Hat Enterprise Virtualization product,” said Hellekson. “They didn't want to train people on two different products and operate two different silos. So, they used our CloudForms product to manage both the VMware and Red Hat Enterprise Virtualization infrastructures. Now, they can compete the virtualization layer of their data center, which will keep costs even lower. CloudForms also let them add resources from Amazon, so they have their legacy VMware infrastructure, the new, lower-cost and open source Red Hat Enterprise Virtualization infrastructure, and all the public cloud resources they need, managed and governed and metered as they need it.”

Cloud computing has been a game-changing development for government agencies. With the use of an open platform, the possibilities for innovation in the cloud become limitless, allowing government agencies to re-think business operations and service delivery.

YOUR CLOUD COMPUTING CHEAT SHEET

Looking to get smart on cloud? Here's a quick primer.
We recommend printing this page out and sharing with your peers – it's a good reference.

THE CLOUD

Cloud is an information technology delivery model that enables on-demand access to resources, whether they are servers, computing power, applications, data or software, which can then be quickly acquired by employees using laptops, desktops or smart phones.

CLOUD SERVICE MODELS

Below are three cloud service models. Examples are provided in Lesson 2 of this report. (See Page 4.)

SOFTWARE-AS-A-SERVICE

An agency accesses software on-demand from a third party vendor. The agency does not buy the software, but is provided multiple licenses to access information.

PLATFORM-AS-A-SERVICE

A vendor provides an online development platform for an agency. Developers leverage the vendor's computing environments and can test, create and ultimately host new applications.

INFRASTRUCTURE-AS-A-SERVICE

A vendor provides the hardware and software, and a government agency can build a customized computing environment. This delivery model can provide government agencies with access to advanced computing power, storage, memory, bandwidth and software applications – all available on demand.

CLOUD DEPLOYMENT MODELS

Below are four common deployment models, explained in depth in Lesson 3 of the report. (See Page 5.)

THE HYBRID CLOUD

Consists of two or more deployment models. For instance, a hybrid cloud will contain both a public and private cloud. It has the ability to easily segment data and transfer data between clouds as necessary.

THE PUBLIC CLOUD

A cloud deployment that makes information available for the public.

THE PRIVATE CLOUD

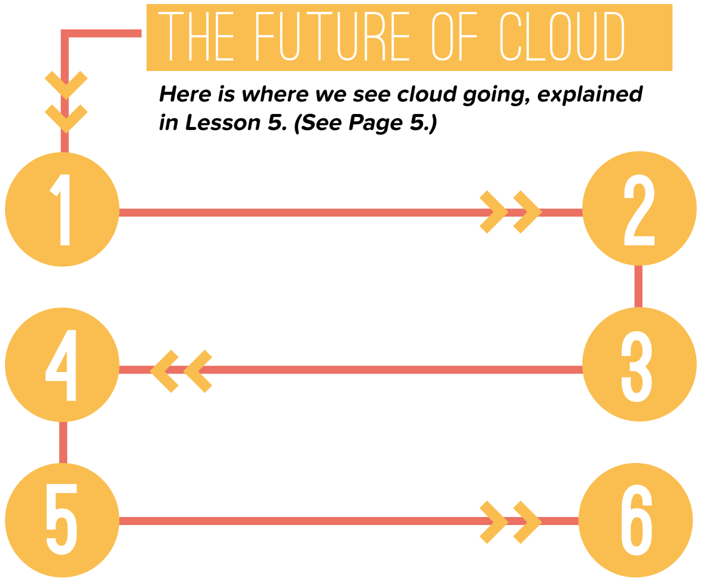
A cloud deployment that is used exclusively for internal applications within an agency, but multiple business units may be granted access to share information and manage data.

THE COMMUNITY CLOUD

A cloud deployment model that provides access to multiple organizations that have a similar interest in collaboration. You may also hear this kind of cloud referenced as a "government only" cloud model.

THE FUTURE OF CLOUD

Here is where we see cloud going, explained in Lesson 5. (See Page 5.)



1 Increased case studies of hybrid and specialized cloud

2 Everything-as-a-service

3 Powering data anywhere, anytime

4 Lighter devices with on-demand access to computing power

5 Internet of Things

6 Leveraging cloud brokers to manage cloud solutions

MAKING THE BUSINESS CASE

Questions to ask. Learn more by checking out the state of Illinois case study. (See Page 15.)

1. What is the current level of risk? What is our risk tolerance?
2. What is the trajectory of risk? How can we manage risk?
3. What does cloud mean for our workforce?
4. What kind of service-level agreements do we need?
5. What kind of SLAs can we reasonably enforce?
6. What do we do at the end of the contract term?
7. How do we address the problem of vendor lock-in?
8. How will these solutions save us time and efficiency compared to traditional methods?
9. How does this transition affect our workforce?
10. Are we solving the right problem? Will this investment facilitate improved service delivery?

BEST PRACTICES FOR CLOUD ADOPTION

A quick list of our best practices. Be sure to view the “Your Best Practices for Cloud Adoption” section. (See Page 23.)

1. Match problems to IT solutions.
2. Navigate cultural barriers.
3. Engage the legal team to understand the evolving environment.
4. Define data ownership.
5. Collaborate and speak the right language.
6. Start small and pilot test.
7. Proactively address security concerns.
8. Provide educational opportunities.
9. Form a small team that meets frequently.
10. Classify your data.

Figure 1:
[Select all that apply]

WE ARE CURRENTLY USING THE FOLLOWING SERVICE MODEL:

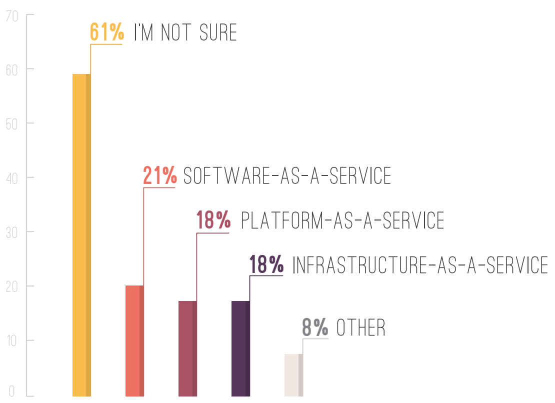
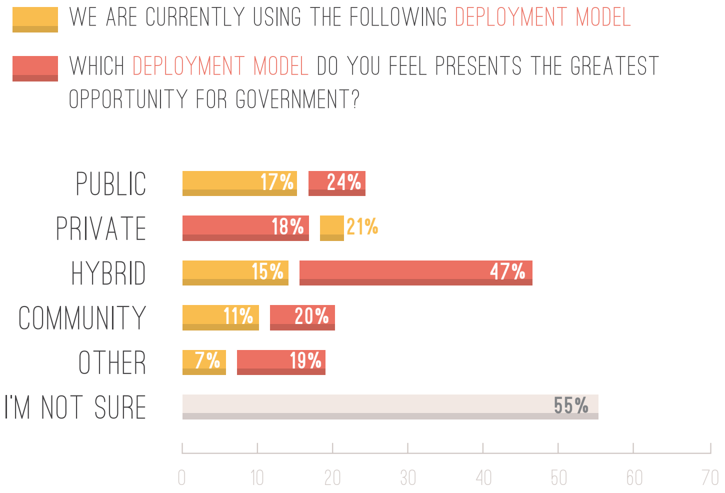


Figure 2:
[Select all that apply]


🟨 WE ARE CURRENTLY USING THE FOLLOWING DEPLOYMENT MODEL

🟥 WHICH DEPLOYMENT MODEL DO YOU FEEL PRESENTS THE GREATEST OPPORTUNITY FOR GOVERNMENT?

WHAT IS A CLOUD BROKER?

Want to know more about a cloud broker? Check out our Texas case study. (See page 14.)

Cloud brokers present many benefits to government agencies. They serve as the intermediary between vendors and government. Due to the complexity of the cloud, one service provider may not be able to meet all the requirements that your agency has. A cloud broker can help your agency create a customized cloud solution. Cloud brokers manage the cloud adoption process and integrate everything into a single location, helping you centrally manage numerous platforms and services.

Although a standard definition is hard to come by, the basic role of a cloud vendor may include some of the following:

» Centrally managing multiple cloud solutions, helping to reduce costs and improving efficiency of IT solutions across an agency.
» Vetting a vendor to be sure that it meets the agency’s security and compliance standards.
» Helping with the quick provisioning of additional services.

Figure 3:

DOES YOUR AGENCY USE A CLOUD BROKER?

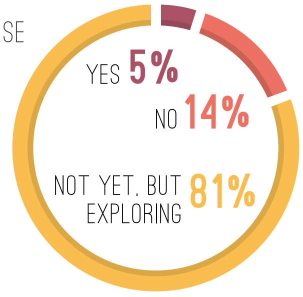
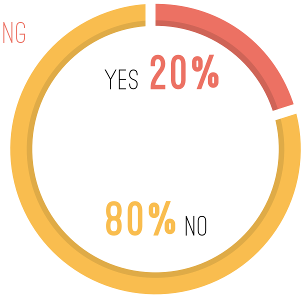


Figure 4:

DOES YOUR AGENCY PROVIDE TRAINING ON SECURELY USING THE CLOUD?



vion.com

STRONG SOLUTIONS IN THE CLOUD.
SOLID SUPPORT ON THE GROUND.

ViON Cloud Solutions has over a decade of experience making the cloud work for government agencies and world-class organizations. Our high-performance enterprise-class system combines the flexibility, efficiency, and power of the cloud with the safety of on-premise installation. Add that to our 24-7 customer care for a cloud-to-ground experience like no other in the industry today.

LEVERAGING CLOUD ADOPTION IN YOUR AGENCY

An interview with Ray McCay, ViON vice president, solutions strategy

Government agencies face a unique set of challenges when adopting cloud. Ray McCay, ViON vice president, solutions strategy, recently spoke with GovLoop about the greatest challenges, best practices and how ViON can help government deploy cloud solutions based on 15 years experience with cloud implementations.

When it comes to adopting cloud technology, the top concern for government, McCay noted, is security. Agencies worry that their cloud environment and internal data could be exposed to the outside. Especially for agencies with confidential data, the probability of a security breach has many officials wondering if cloud is worth the risk.

Another concern? Implementation. For some agencies, moving to the cloud means procuring new IT solutions and conducting a complete overhaul of existing systems. "You have a lot of legacy systems that make it difficult to even be able to implement a cloud system," said McCay. "A lot of the procurement cycles and contract vehicles are not able to handle a more dynamic approach to IT services which the cloud offers. There is a need for procurement education to share ways to write contracts so the government benefits from new consumption models. You may have to create brand new contracting vehicles which are complex and may delay deployment."

Despite these obstacles, agencies continue to adopt cloud solutions, often because the cloud offers lower costs and more flexibility than traditional, on-site IT enterprises. Instead of owning the entire infrastructure, cloud allows customers to pay as they use it. Furthermore, there is a wide range of cloud enterprise solutions available – an agency can choose from public, private, or hybrid cloud systems.

So how does an agency identify the most suitable cloud solution? McCay offered a set of best practices when considering cloud. First: assessing your agency's data needs is paramount. "The first thing to do is to start by gaining an understanding of what problem you're trying to solve, and realizing right up front that not all clouds are created equal," said McCay.

He recommends public cloud for agencies with lower security requirements or open data that can be shared with the public. A private cloud, or a cloud model that is accessible only to a specific agency, may be what is needed in some cases by to fully protect their data. ViON's private cloud solutions place the cloud infrastructure behind a customer's firewall, ensuring a higher level of security.

Agencies must also identify their application requirements. For example, an application that hosts live satellite feed data over North Korea utilizes a different infrastructure than an application that shares medical images between hospitals. "Not all applications are equal. Figure out what it is you need to be successful," McCay advised.

To leverage cloud adoption, McCay recommended partnering with a cloud vendor that offers flexible solutions and prioritizes organizational needs. ViON cloud services combine a customer-first mission with a variety of cloud solutions – including Tier One and Capacity Services – to provide agencies with the best cloud solution. ViON has been implementing cloud services for over 15 years with high customer satisfaction.

"Our legacy is to focus on the hardest problems, the biggest scale issues, the toughest performance issues, the most critical application environments, and deliver infrastructure that will thrill our customers," McCay stated.

Adopting a new data infrastructure is not an easy task. Finding the right vendor and identifying agency data and application needs can make a daunting mission of switching to cloud possible.

ACKNOWLEDGEMENTS

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 100,000 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 send us an email at: founder@govloop.com

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

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

www.govloop.com
Twitter: @GovLoop

SPONSOR ACKNOWLEDGEMENTS

Thank you to Akamai Technologies, Amazon Web Services, Avnet, Brocade, DLT Solutions, GovDelivery, NetApp, Presidio, Red Hat and ViON for their support of this valuable resource for public-sector professionals.

Authors: Pat Fiorenza, senior research analyst.

Designers: Jeff Ribeira, senior interactive designer, Tommy Bowen, junior designer, and Maddy Haigh, design fellow.

Editors: Steve Ressler, president and founder, GovLoop; Catherine Andrews, director of content, GovLoop.

1101 15th St NW, Suite 900
Washington, DC 20005
Phone: (202) 407-7421
Fax: (202) 407-7501