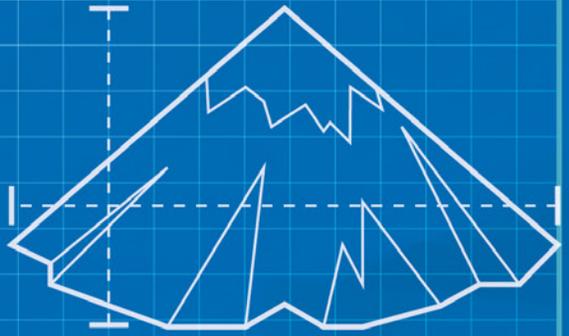
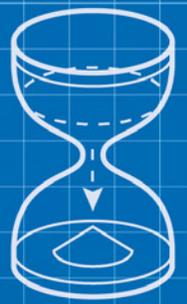
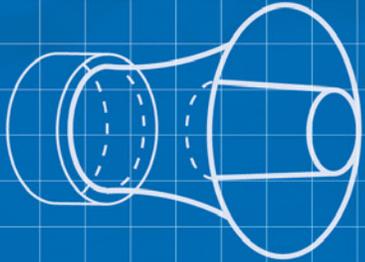
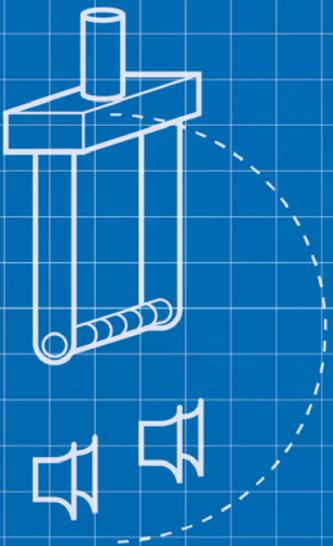
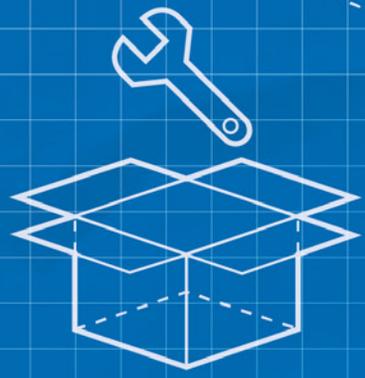
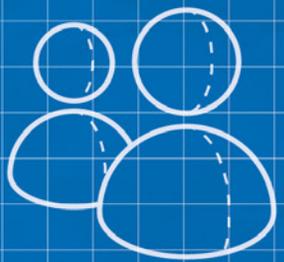
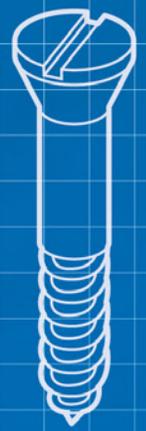
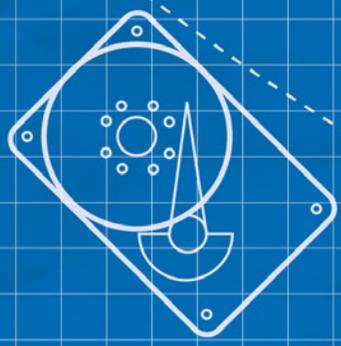
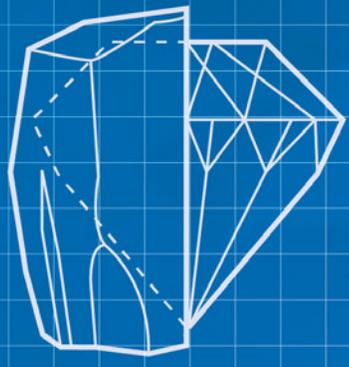


# Your Guide to Using Everything-as-a-Service



# Everything-as-a-Service (XaaS)

[n. zas]

A strategy of using cloud offerings and service models to create a holistic, streamlined IT infrastructure.

# Executive Summary

# Contents

A 2012 study reported that the government saved \$5.5 billion by switching many of its local technology services to the cloud. However, that figure pales in comparison to a potential \$12 billion in savings.

So what caused this large gap in realized savings? Hesitance to adopt cloud solutions and difficulty securing offsite information were main factors – but there was another unexpected issue. These cloud solutions, while saving costs in some places, were also adding complexity to government networks and hindering many processes from reaching maximum efficiency.

Network complexity continues to be a barrier to realizing the full potential of cloud offerings. As a result, even as cloud solutions help transform government, they're creating new challenges and, in some instances, preventing government from adopting cloud solutions at all.

GovLoop surveyed its public sector audience to determine how their organizations are adopting cloud models. "With the infrastructure currently in-house, I am not sure the cost-to-benefit ratio is high enough to move to the cloud yet," one respondent said.

Current infrastructures should not be a barrier to cloud transitions, nor should cloud transitions disrupt your existing information technology architecture. To ensure that cloud adoption maximizes its benefits without decreasing the efficiency of the organization, agency officials must craft a holistic strategy before deploying new service models.

In this guide, we explore this strategy of using everything-as-a-service (XaaS). This guide will:

- ▶ **Explore the benefits of XaaS models.** Adaptability, efficiency, and cost effectiveness are just the beginning. Learn how cloud service models can help you elevate your agency's performance.
- ▶ **Consider the risks of cloud integration.** Concerns about data privacy and accessibility come with any cloud deployment. XaaS, however, also requires understanding how new applications may improve or disrupt your current processes.
- ▶ **Prescribe a roadmap to your appropriate XaaS strategy.** There is no one-size-fits-all way to maximize XaaS applications. Determine how to use the cloud in a way that reaps the benefits of service without compromising your data, processes, or security.

By explaining the basics of XaaS strategies and highlighting case studies from the public sector, this guide will give you a framework to consider effective cloud service model implementation at your agency.

2	Executive Summary
3	What is Everything-as-a-Service?
4	XaaS in Action
5	3 Ways to Make Better Cloud Decisions
7	The Challenges of Cloud
8	The Benefits of Using XaaS
10	Planning Before, During, and After Cloud Deployment
11	Forming a XaaS Strategy
13	Preparing Your Agency for Cloud
16	Creating a Single Government Cloud Strategy
17	The ABCs of XaaS
18	Executing XaaS Strategies
20	Using Cloud Today... And Tomorrow
22	Traps to Avoid When Implementing Cloud
23	XaaS is Not Always Cloud-First
26	Easing the Transition to XaaS
27	The Impact of XaaS on Procurement Processes
29	Planning Guide
30	Acknowledgments



# What is Everything-as-a-Service?

The phrase “Everything-as-a-Service” can be confusing because people in the tech industry often use it in divergent ways. Our recent survey of public sector professionals confirmed this diversity of interpretations. Some simply use the phrase to describe the multitude of cloud offerings available to replace locally designed and owned services. Others use everything-as-a-service, and especially its acronym XaaS (pronounced “zass”), as a catchall to describe any cloud service model, such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or and Infrastructure-as-a-Service (IaaS). Finally, we occasionally hear XaaS used to describe the merging of public, private, and hybrid cloud offerings.

## Definitions from the GovLoop audience

- ▶ “Cloud-based operational software, interfaces and data management.”
- ▶ “An IT application that is pay per use.”
- ▶ “Outsourcing services... paying a smaller fee for someone else to do the skilled technical pieces.”
- ▶ “Instead of a system where it is developed, managed, maintained by a government entity, all these tasks are procured by a customer to a group, subgroup, or entire organization.”
- ▶ “Externally purchasing services and capabilities on an ongoing basis as an operating expense to the business, as opposed to a capital expense.”

These definitions aren’t incorrect, but they miss a crucial piece of the cloud puzzle: interoperability. Within this guide, we focus on the strategy of XaaS. In other words, we think about effectively using everything-as-a-service, and what that means for your agency’s cloud purchasing and deployment strategy.

**Everything-as-a-Service (XaaS)** — *A strategy of using cloud offerings and service models to create a holistic, streamlined IT infrastructure.*

## Cloud à la carte

An analogy may be helpful. Consider going to a restaurant for dinner. Rather than choosing a prix fixe menu, you create your own meal by choosing several selections from an à la carte menu.

There are a number of considerations to keep in mind as you choose what goes into your meal: Do you have any allergies that preclude you from choosing certain items? What menu items do you already know to be tasty or filling? Is everything going to fit on the plate you are given? Most importantly, will each of the items you choose complement the other selections in your dinner? For instance, you probably aren’t going to pick a slice of pizza to go with your filet mignon. At the end of your decision-making process, you want to ensure your dinner is still a complete and tasty meal, despite it being put together piece by piece.

This is what IT professionals are being asked to do when they acquire new cloud services. No single cloud application can replace an organization’s entire IT system. Instead, technology professionals must add individual cloud offerings to their infrastructure to create a cohesive network of systems.

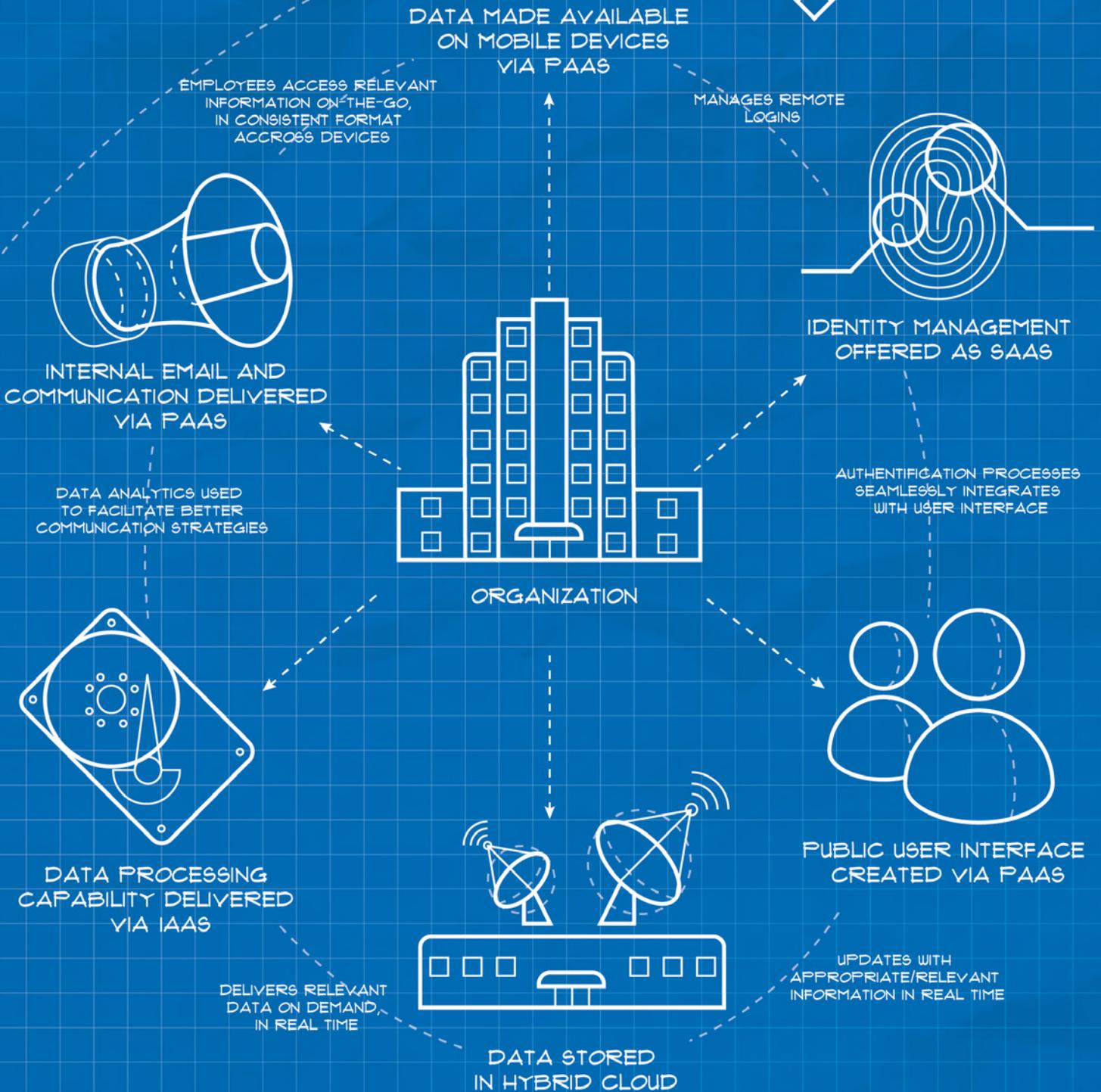
In doing this, IT must have similar considerations to a diner piecing together a meal. They want to make sure new services are compatible with current systems. They also want to choose trusted vendors with solutions proven to work. Finally, IT managers want to make sure they aren’t adding unnecessary complexity to their organization’s processes.

The end goal is an architecture that effectively uses everything-as-a-service, and that goal should guide each step of cloud procurement and deployment.

XaaS, therefore, is not the cloud. Nor is it buying a complete SaaS or PaaS offering. Instead, it’s a way of creating an IT infrastructure that incorporates cloud offerings — whether they are bundled or sold separately; public, private or hybrid; custom or off-the-shelf — in a way that increases operability without adding complexity to systems.



# XaaS in Action



# 3 Ways to Make Better Cloud Decisions

An interview with David Blankenhorn, VP of Engineering and Chief Cloud Technologist at DLT Solutions

Before acquiring cloud technology, rigorous scrutiny is required to ensure the proposed solution is actually the best fit for a government organization's IT needs. To discuss the necessary components of this scrutiny, we spoke with David Blankenhorn at DLT Solutions, a value-added cloud reseller with over 23 years of public sector experience. He outlined three ways that DLT helps agencies make better cloud decisions: education, training, and affinity mapping.

Blankenhorn asserted that government organizations shouldn't assume cloud models are the right answer to any technology need. "Cloud computing is just another set of technologies that customers can use to help satisfy their mission requirements," said Blankenhorn. "It's another tool that's available, and like any tool you need to understand the proper way to use it. You have to take a hard look at your requirements, and by evaluating those requirements against the tools at hand, you come to the right solution. Sometimes it's cloud, and sometimes it will be more traditional designs."

Blankenhorn suggested using a multi-criteria decision analysis matrix to correlate the capabilities of the various cloud and traditional platforms to the key requirements. This tool can quickly identify the platforms that are good contenders for hosting your application.

While the matrix itself is a simple tool, ensuring that it is effectively utilized is more challenging. Education is key. "The trick is filling it in correctly in the first place. You have to understand the technology that you're dealing with. If you don't have a fair

and accurate representation of the platform's capabilities, you'll get a lot of false negatives," said Blankenhorn. "A large part of our engineering team's time is dedicated to helping our customers understand the capabilities of the cloud platforms, what their options are, what the best fit is, and equally important where it's not a good fit."

DLT Solutions commits significant time to educating customers about the possibilities of cloud. Blankenhorn said, "One of the biggest dilemmas preventing wider cloud adoption is just the lack of understanding. There is a considerable lack of experience, and a number of folks who are managing or designing IT systems within the public sector have had limited exposure to cloud technologies."

Additionally, DLT trains potential cloud adopters to fully leverage cloud. "If they're not properly trained, then they're not going to be able to properly administer, monitor, or manage those environments," said Blankenhorn. "For example, they may be great at managing a virtual machine running in the cloud environment. But if they don't truly understand how the platform works and how to take advantage of the tooling that's native to the platform, then they're only seeing part of the picture."

Lastly, DLT ensures that cloud customers understand how a new solution will interface with the rest of the organization's IT infrastructure. Blankenhorn stated, "There is a level of integration that needs to take place with most modern applications. I don't see anybody moving an entire agency into a single, homogenous cloud infrastructure.

The challenge you have to deal with is making sure that you have clear connections between your cloud solutions."

Affinity mapping, a method used by DLT, is a process cloud adopters should use to determine how an application interacts and relies on other applications or systems within the environment. This takes place before an agency commits to deployment.

"We've run into situations where an application shouldn't be moved because of some dependency that the application has on some other IT system. Had we moved that application, unexpected latencies may have rendered that application – or a related one – unusable," said Blankenhorn. "That's why one of the first things we do when we are evaluating a workload for migration to a cloud is an affinity mapping. Just to make sure we know what all the other systems are that the application needs to talk to before we move that out to the cloud."

Scrutiny is necessary but it shouldn't deter cloud adoption. Instead, scrutiny ensures that technology needs match capabilities. Blankenhorn affirmed, "What we bring to the table is a robust portfolio of cloud technologies that we can apply to a customer's needs. In some cases we've even synthesized new solutions like DLT's CODEvolved PaaS to meet our customer's mission requirements."

To ensure that a given solution is actually appropriate requires agencies to execute informed decision analysis, learn the nuances of a solution's potential, and map the solution to the rest of the infrastructure.



# CODEvolved

Capacity on Demand. Evolved.



**A rapid private Platform-as-a-Service environment for application development, testing and hosting built entirely in the cloud.**

- No Upfront Capital Investment
- Scalability
- Decreased Lag Time
- Privacy & Security
- Familiar Programming Languages & Tools
- Operational Speed & Agility
- Reduced Waste

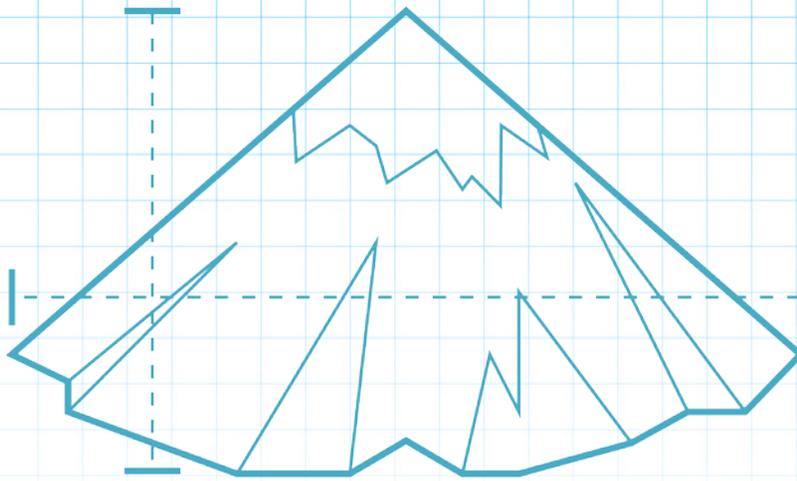


<http://www.dlt.com/CODEvolved>



DLT SOLUTIONS®

# The Challenges of Cloud



Transitioning one service at a time to the cloud may save your agency money in terms of startup costs, maintenance, and usage fees, but it doesn't necessarily simplify your IT logistics if cloud services aren't creating a holistic system. In fact, haphazardly transitioning to the cloud service by service could increase the complexity of your IT infrastructure. According to a MeriTalk survey, more than 50 percent of agencies said the complexity of their IT networks increased in the past year.

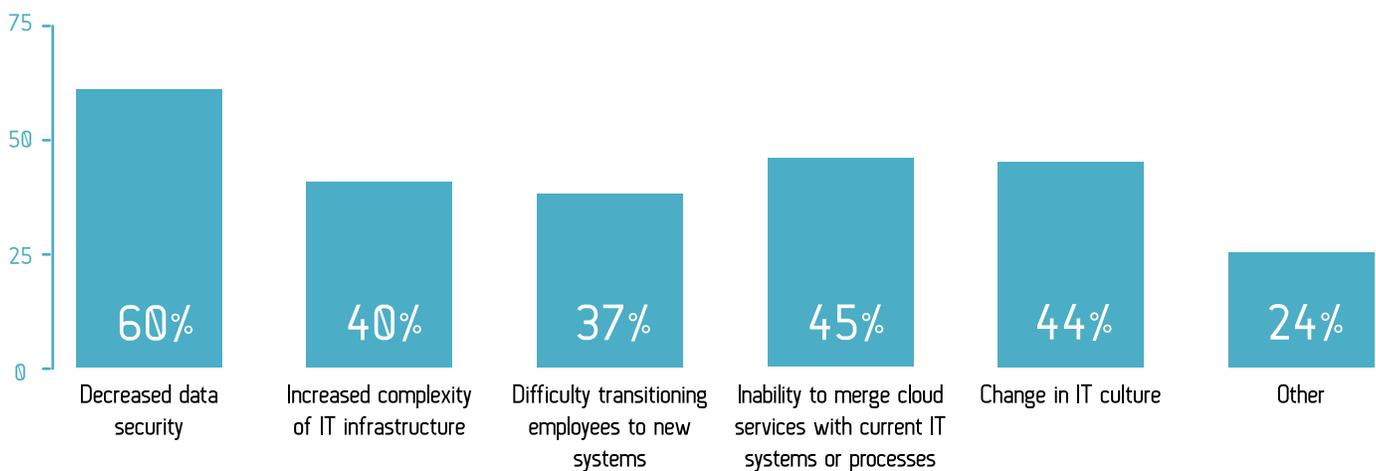
Deploying piecemeal cloud solutions to your IT system without first creating a XaaS strategy can negatively impact your organization at every level.

Internally, your employees may face fresh barriers in connectivity and productivity if new cloud solutions aren't properly integrated into their existing processes. There is also a risk of employees being unable to use services if new systems are deployed too quickly and without proper training opportunities.

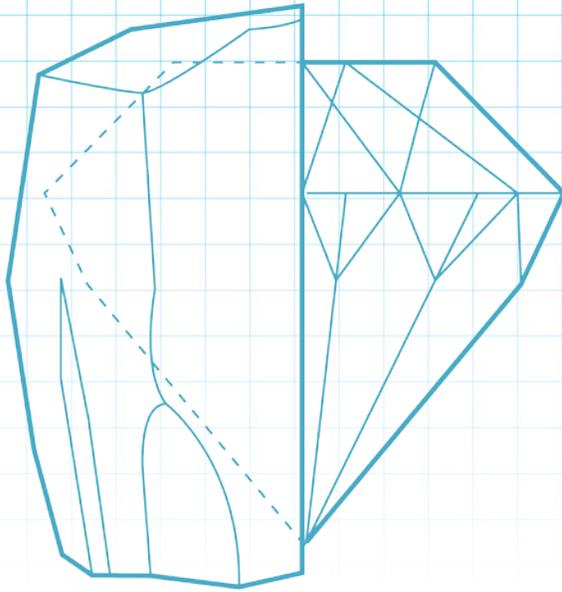
On an organization-wide level, you risk creating a network that is un navigable and disconnected. The "Presidential Directive for Records Management" mandated that all agencies fully manage permanent records in an accessible, digital format by 2019. That means that within five years there's going to be an exponential amount of information that can be accessed only through your IT network. If that network is built without a cohesive strategy, the likelihood that information will be lost or improperly managed is high. Moreover, increased network complexity may prevent different departments from effectively communicating and collaborating via technology.

Finally, even as cloud offers greater mobility and enhanced data capabilities, a disparate cloud network can make it more difficult for the public to access your resources. If public-facing digital services do not interface with one another, or if they aren't accessible from a central platform, public users will be unable to take full advantage of your online services and resources. Citizen engagement may suffer as a result.

What risks do you anticipate when considering cloud services as replacements for local systems? (check all that apply)



# The Benefits of Using XaaS



The benefits of cloud services are innumerable. Our recent GovLoop Guide, [Cloud Computing: How Cloud is Reinventing Government](#), explores many of them in depth, but here's a quick refresher.

## Cloud services can:

- ▶ Lower costs by saving on data storage, processing, and implementation.
- ▶ Decrease time and labor requirements for technology transitions.
- ▶ Increase efficiency by providing easier access to secure files.
- ▶ Offer greater mobility to employees and the public.
- ▶ Update automatically and lower maintenance requirements.
- ▶ Drive collaboration by creating shared tools and infrastructure.

An ad hoc deployment of disparate cloud offerings can easily diminish these benefits, however. XaaS is a way of holistically transitioning to the cloud that reduces the complexity of IT on your end, while maintaining or improving the performance of your services. Creating a strategy before deploying individual cloud platforms is essential. If you execute a XaaS strategy, you can expect significant gains. An effective strategy should yield:

**Agility.** Cloud technology can be swiftly acquired and deployed to meet emerging needs. However, IT managers should take care to guarantee that new solutions don't create new problems. A XaaS strategy is not meant to inhibit an IT infrastructure from creatively adapting. Instead, it ensures that when an appropriate cloud solution is available, it can be more seamlessly integrated into the existing architecture.

**Cost containment.** Cloud services reduce costs by allowing users to pay only for the bandwidth used. A XaaS strategy builds on these cost savings by further ensuring that services aren't duplicative or decreasing productivity through added process complexity.

**Efficiency.** Because it ensures that solutions effectively interact with one another and with local technologies, a successfully deployed XaaS strategy will guarantee that all of the benefits of cloud's speed, productivity tools and user ease are realized on an enterprise-wide level, rather than just within each solution.

**Collaboration.** Using everything-as-a-service goes beyond deploying individual collaboration or mobile solutions. It creates a standardized network across your organization — and across your various cloud solutions — that makes sure any collaboration tool will be operable in any setting. Therefore, the benefits of a single

communication platform can be extended beyond a single department to interact with other platforms and employees across your agency.

**Security.** Sixty percent of respondents to our survey said that security concerns were a major consideration for transitions to cloud services. However, [according to the National Institute of Standards and Technology \(NIST\)](#), cybersecurity can be drastically improved by creating a streamlined cloud environment. A homogenous infrastructure can help IT managers more easily identify and address potential threats and irregularities. Moreover, a uniform environment allows for automation of many security management activities.

**Engagement.** A seamless interface that incorporates multiple cloud solutions allows the public to easily access your digital resources. XaaS strategies go beyond simply purchasing platform or interface cloud bundles. Instead, XaaS consolidates and streamlines various cloud services, either bundled or separate, into a single process map. The public can then use your services with confidence, knowing that they are accessing the full spectrum of your offerings and that each solution will work with others.

# MOVING YOUR AGENCY INTO THE CLOUD...

## IT'S OUR BUSINESS.



**ViON**   
Building your enterprise solutions

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.

In partnership with

 **Hitachi Data Systems**  
Federal Corporation

[vion.com](http://vion.com)

# Planning Before, During, and After Cloud Deployment

An interview with Rob Davies, Vice President of On-Demand at ViON

Government agencies are experts in planning. Budgets, hiring, and a multitude of other tasks are scheduled and meticulously planned well in advance, in order to secure the necessary resources to achieve mission goals. But fewer organizations have extensive experience in planning for cloud transitions.

Rob Davies from ViON, a veteran cloud provider to government organizations, asserted that cloud deployment requires just as much planning as your annual budget proposal.

“Cloud is just like any other technology project,” Davies said. “You have to do due diligence with respect to planning, testing, and investigating.”

This sort of scrutiny is crucial. “If you haven’t planned carefully and executed the testing in your cloud service provider’s environment, the solution might not work the way you want it to,” said Davies. “In many cases with the federal government, it’s trying to make something more readily accessible to the citizenry. If it doesn’t work, that’s going to cause a lot of rework and unplanned costs.”

Before executing a cloud deployment, agencies must assess their current state and future goals. “What components or parts of their workload are they looking to migrate to cloud?” asked Davies. “Have they completed an analysis of their entire workload?” Without an adequate view of these considerations, organizations may deploy a solution that does not align to their strategic goals, and consequently produce the desired results.

Given current infrastructure and needs, an organization should create a budget to match its goals. This budget should not only include transition costs, but also the potential costs of moving from the cloud solution.

“Another consideration is, once a contract’s up, what’s my transition out approach? What are the associated costs or budgets that I might need to establish?” said Davies. “You always have to have a transition plan for that contract, and cloud isn’t any different. Just, hopefully, the technology makes it a lot easier to go through that process.”

Once you’ve asked the right questions, your agency will need to focus on finding the right answers. “The key is to find a partner that has the knowledge and experience in providing cloud solutions, who can identify potential pitfalls in the planning stages, so they don’t become realities,” said Davies. “When you look at cloud solutions, you have to make sure they run on the platform, they are in the right language, they require minimal work, they have the right security profile – there is a lot to consider.”

In many cases, cloud transitions will require melding cloud offerings with legacy systems, either due to contract constraints or because those systems are necessary to the overarching IT infrastructure. “Getting everything to the cloud doesn’t mean getting everything to a cloud service provider,” said Davies. “There’s a tremendous amount of government workload that runs on legacy systems which means the cloud solution needs to integrate seamlessly with the existing platform. It may also mean bringing the efficiencies of the cloud to the agency. That sounds straightforward, but there is a lot of work that goes into that.”

In addition to checking for integration capability, agencies must ensure that whichever cloud configuration is chosen will also meet the transparency and auditability standards necessary of government IT systems. “You have to make sure the provider is delivering a supported cloud in the federal space that is built around acquisition regulations,

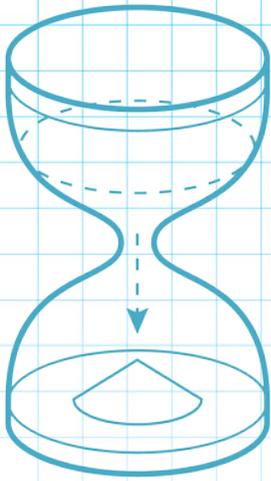
standards, and the deliverables that the government requires,” said Davies.

Finally, cloud solutions should be considered for their ability to adapt. In addition to matching a cloud solution to the demands of your agency today, consider its ability to scale with agency growth and integrate with the next wave of technology innovations. Once your cloud solution is deployed, it should be continuously adapted to meet both short and long-term planning goals. This may require working with your cloud provider to alter processes and configurations, as business needs change.

“If you’ve got a specific system or project you need help with, we’ll sit there and show you how to do it in real time,” Davies said. “When ViON started as a solutions provider for government, we provided the services to help architect, configure, stand-up and then be available for questions while it was running. We viewed it as part of our responsibility and business model to have that expertise available. That carries over into cloud today.”

Throughout the lifecycle of a cloud acquisition, careful preparation is required to avoid unplanned costs or service disruptions. An optimal cloud service provider not only delivers solutions, but also makes sure they are deployed with appropriate scrutiny.

“It’s a different technology platform and capability, but that doesn’t mean that you can skip your planning and your budgeting and your contingency planning,” said Davies. “Agencies must consider the full picture of what they’re going to put in the cloud, how they’re going to manage it when it’s in the cloud, and how they are going to operate as an organization once their application is in the cloud.”



# Forming a XaaS Strategy

Few doubt the advantages, and even the inevitability, of the transition of government IT services to the cloud. Now, the conversation has changed from what we can gain from the cloud to how we can reap those benefits.

So how do you get the most out of cloud solutions? There are four steps to creating a XaaS strategy that won't disrupt or complicate your current IT infrastructure:

## 1. Analyze your current infrastructure

Some organizations may already have a detailed understanding of their current IT infrastructure. Others will need to take time to map the processes, solutions, and networks that comprise their IT system. In either scenario, it's crucial to begin your journey to a XaaS strategy by examining your current infrastructure.

In addition to cataloguing the solutions already deployed at your organization, there are a number of factors to consider in your analysis. To determine how your IT architecture operates, you must also think about current operating costs, connectivity with other agencies, contractual obligations to current systems, and operating efficiencies. Additionally, make sure you are not only analyzing what comprises your system, but how various systems interact with one another and with users, both internal and external.

Finally, don't exclude current cloud solutions from your analysis. By now, your organization has likely already acquired some cloud services. In a recent GovLoop survey, more than 60 percent of respondents reported that their organization had transitioned at least some IT services to the cloud. However, that doesn't mean it's too late to form a coherent XaaS strategy.

If anything, these early cloud acquisitions can actually advance your new XaaS strategy. Analyze how they interact with your current infrastructure: Are they complicating your network? How could you get more from the solutions already deployed? Use the successes and setbacks from previous cloud transitions to determine how your agency is currently leveraging the cloud.

## 2. Set an end goal

Once you've determined how your architecture operates, scrutinize if its current state meets your organization's needs. Rather than trying to identify specific processes that can be altered, start by considering an ideal IT architecture broadly. On a high level, what do you want your organization to achieve through technology? Create an ideal profile for what that looks like. This is your end goal.

Take caution, however. Although your end state should be forward thinking, it should also be realistic. It's important to account for the constraints of your organization, including its IT capabilities, purchasing processes, security concerns, and appropriations restrictions. These concerns may hinder your ability to adopt cloud solutions and should be addressed before a cloud strategy is executed. For instance, many cloud solutions require greater data storage and processing speeds. Consider what your current architecture can support and what capacities you may need to add before transitioning to cloud.

## 3. Determine your XaaS strategy

A strategy that guides all, rather than individual, cloud purchases and deployments is necessary to ensure that any new solutions will seamlessly integrate with your current infrastructure.

Your strategy won't necessarily be a step-by-step guide, with every new cloud solution predetermined. But it should include guidelines for what processes will be moved to the cloud and what characteristics should be streamlined across adopted solutions. Moreover, it should include a basic timeline that directs which services will be transitioned first and over what period of time transitions will take place.

Most importantly, your strategy should incorporate your entire IT architecture into every facet of planning. The section, "Executing XaaS Strategies," offers detailed guidance on how to ensure seamless transition. For now, it's important to realize that any cloud strategy can be effective only if it takes a holistic approach.

## 4. Communicate your strategy

This step is most often overlooked. More than 65 percent of respondents to our recent GovLoop survey said they were unaware of the strategy used to procure cloud services at their agency. Yet ensuring that everyone, both internal and external, understands your organization's strategy for cloud transition is crucial. It will guarantee that solutions adopted in any one department are checked against organization-wide standards and procedures. It will also better prepare the public for changes in your processes, which may affect them.

# PRESIDIO

Practical thinking for a connected world.

---

## ADVANCED FEDERAL IT SOLUTIONS TO ENABLE INNOVATION, SECURITY & AGILITY.

---



We think about, architect, implement, and support the practical reality of advanced technologies every day. We are not just trusted partners, we enable new thinking.

For years, that “new thinking” has allowed Presidio’s Federal Team to revolutionize the Federal Government by providing access to an evolving breadth of advanced technologies that are emerging and innovative.

---

To learn about our Advance IT Solutions visit  
[HTTP://WWW.PRESIDIO.COM/GOVLOOP](http://www.presidio.com/govloop)



# Preparing Your Agency for Cloud

The FCC's plan to meet the next decade of technology demands

**No two agencies are alike.** Therefore, no two XaaS strategies should be the same. Both your agency's current IT environment and needs for the future should determine how the organization adopts cloud. Dr. David A. Bray, Chief Information Officer at the Federal Communications Commission (FCC), described how his agency plans to transition more than 50 percent of its IT to the cloud within 24 months, despite the reality of a small IT workforce and several legacy technology systems.

## Identify Cloud Needs

When Dr. Bray took his post at the Commission in August 2013, there were 207 locally hosted technology systems in operation. Over 50 percent of those were more than 10 years old. After discussion with the different FCC stakeholders, Dr. Bray determined, "That's not sustainable for an agency of only 1,750 people. We need to modernize so we can spend less of our budget maintaining these agency systems."

In working with his team, Dr. Bray decided an exponential "jump to the cloud" was the answer. "Rather than spending a lot of time, energy, and resources modernizing each

of those 207 systems... we want to create a cloud-based, common data platform," Dr. Bray said.

Moving to the cloud will be cheaper than individual updates to the locally hosted IT systems. It will also allow the agency to outsource some labor-intensive tasks, such as cybersecurity and IT updates, to cloud providers who can better handle this work at a larger scale. Even though administrators will still have to oversee these duties within the FCC, their ability to perform them will be enhanced by leveraging the larger staff and budget of private cloud vendors.

## Prepare for Cloud

Within the next two years, Dr. Bray wants to transition 50 percent or more of the Commission's services onto the cloud. But before the FCC embarks on this ambitious plan, Dr. Bray said they needed to prepare the IT environment to support cloud.

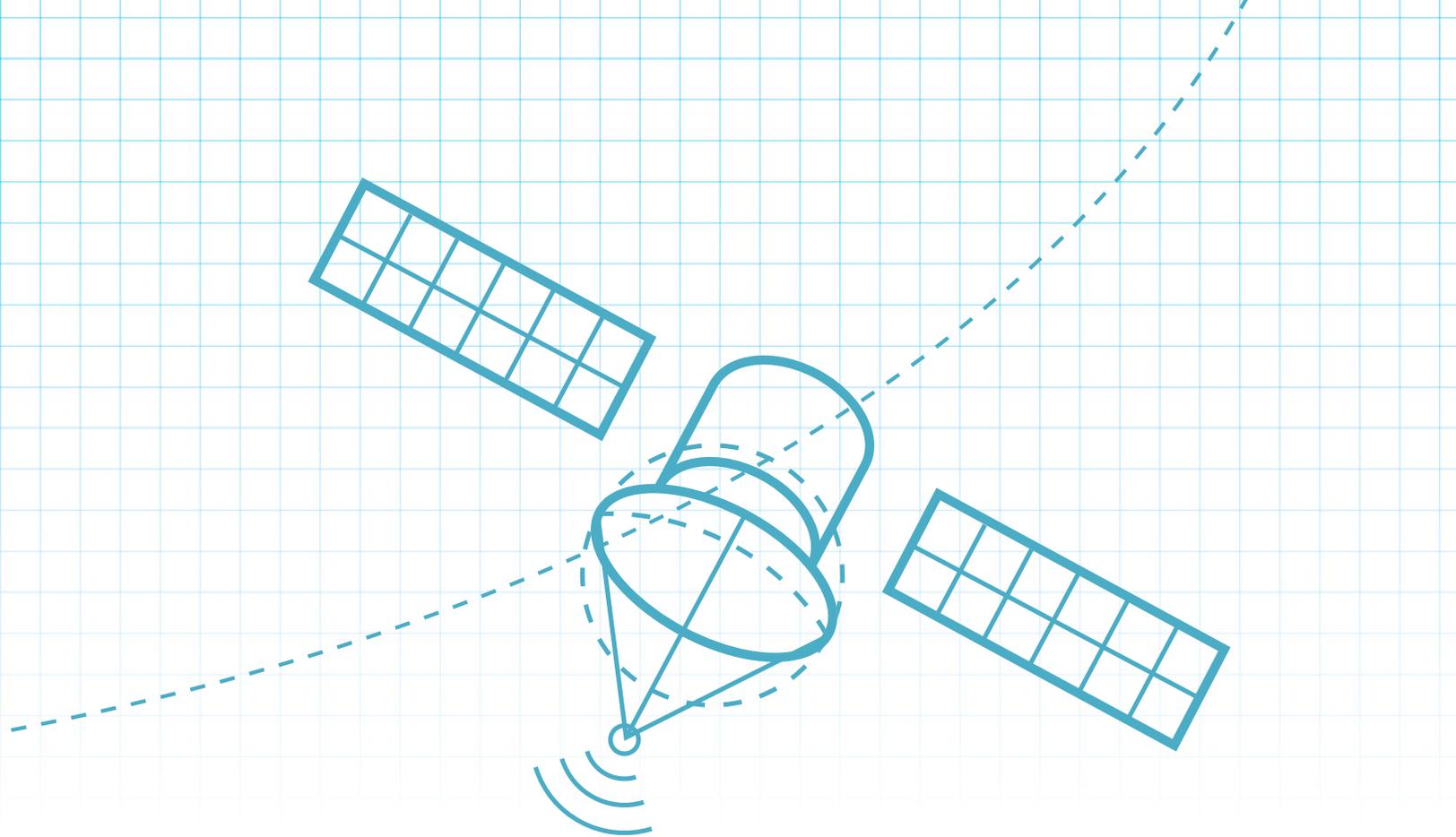
He explained, "Our short-term plan will focus on stabilizing the infrastructure. Before the end of Q2 FY15, we will move the physical servers that we have here at the FCC offsite to a commercially managed

services vendor. We then want to be able to lift our data off these servers to a cloud platform and build on top of that a thin user-interface and reusable, modular code. To help the organization make that transition, the first step is to make it so it doesn't matter where your servers are. We already made the desktops at the FCC virtual to prepare for this transformation."

In addition to adapting his infrastructure, as CIO, Dr. Bray must work to prepare his workforce for new cloud technologies.

"In some respects, moving to cloud is like taking a Cessna and trying to retrofit it to be a 747 in midflight," Bray said. As the FCC's IT systems are replaced, the Commission at-large must continue to operate. To make sure this happens, Dr. Bray created three positions: a deputy in charge of existing technology, a deputy to build the new infrastructure, and an Executive for Modernization to coordinate between the two. These three employees will provide the oversight necessary to transition without major disruptions to the Commission's on-going activities.

Additionally, Dr. Bray emphasized the need to communicate changes to his staff before deployment. He said, "I think that often



times when you're talking about modernization, people gloss over that this is also about loss." The average employee at the FCC has been there for 15.5 years, so they have likely helped build the systems and processes that will be replaced by cloud technologies. Seeking their buy-in, managing the difficult changes ahead, and preparing them for the transition, are just as crucial to success as the technological aspects of infrastructure adaptation.

## Transition to Cloud

Once the Commission's infrastructure and employees are prepared, the next phase of transition will commence. Dr. Bray explained, "The longer-term, 24-month plan will include the shift of data to the cloud-based, common data platform and the rewrite of legacy systems as processes on that platform."

To prioritize which systems will be

transitioned first, Dr. Bray is considering three factors: which systems are identified as most important to the FCC's mission; which systems are in most urgent need of replacement due to advanced age; and finally which systems when migrated will have modular, reusable components that will benefit the migration of other systems as a service.

This last factor will form the basis of the new cloud architecture. Dr. Bray explained, "These components will then allow us to rewrite to a set of systems as modular, building-blocks. We'll have a service catalog of these different components, so that when I do another system that has similar components, I don't have to write them from scratch again. Wherever possible we want to adapt open source components or leverage commercially available solutions vs. write our own code." This building blocks approach will save both time and effort in the transition.

Finally, as the FCC moves to cloud, Dr. Bray will guarantee users have a guiding voice in the transition. He said, "The ultimate test of any good CIO is how well you can take the time to listen, to understand, and to incorporate the different viewpoints of programmatic stakeholders, both internal to your agency as well as external, and also the multiple perspectives of the IT people who are helping make it happen."

Dr. Bray described his mission as, "ensuring that the FCC has sustainable IT for the opportunities of the next decade." For his agency, cloud is the most appropriate solution to meet coming technology needs. However, the ambitious transformation that Dr. Bray has envisioned will only come to fruition as a result of thoughtful, stakeholder-informed consideration of his specific agency's IT and personnel challenges.



# Microsoft Cloud for Government



## Why Microsoft

Designed for government, the Microsoft Cloud for Government is the most complete in the market, offering one solution for productivity, platform and business applications. With familiar productivity tools and single sign on, government employees can get more done, plain and simple. Microsoft Cloud for Government solutions are available from virtually anywhere, on any device.

The Microsoft Cloud for Government provides a common set of security standards, designed to meet rigorous requirements set by FedRAMP controls, which also help customers comply with HIPAA. Choose which workloads should run in the public cloud, government cloud or your own datacenter. With an open and secure platform, Government organizations have development flexibility and the freedom to do more.



## Act Now

- Learn more about the Microsoft Cloud for Government
- Read Transforming Service in the Cloud with Microsoft Dynamics CRM Online for Government
- Visit the CRM App Store
- Sign up for the Azure Government Preview
- Sign up for an Office 365 trial

# Creating a Single Government Cloud Strategy

An interview with Chris Niehaus, Senior Director of Microsoft's National Cloud Computing Program

Cloud is often construed as the next big revolution in government IT. While many in government are on board with the technology, it can still be a frightening enterprise for government entities that have spent tens of billions of dollars building a very robust enterprise and mission critical IT platform.

To support governments in achieving mission success and exceling at cloud implementation, we spoke with Chris Niehaus of Microsoft about how they are helping agencies take the greatest advantage of what they own today, and get the best return on investment.

"We want to provide government a roadmap of how they can extend their services to the cloud, as opposed to ripping and replacing to the cloud," Niehaus explained.

Niehaus said that in order to soothe government agencies' concerns about transitioning to cloud, providing a step-by-step strategy is essential.

"At Microsoft we create a roadmap that says, while you move your email and other elements of productivity to the cloud, you can still seamlessly integrate with your on premise investment so that your users experience one hybrid mission critical platform" Niehaus explained. "In my opinion, that takes a lot of the fear and uncertainty out of moving to the cloud."

A roadmap strategy also allows agencies to maintain control, Niehaus said. "The mission of government is unique across different agencies, whether it's Department of Defense, or whether it's U.S. Department of Agriculture. But they all need to have the

ability to maintain control of those mission critical systems, while still extending the cloud and getting greater return on investment by leveraging across platforms."

Niehaus also explained that since cloud services are often so fragmented, customers can become confused when dealing with the variety of services available. This is why Microsoft provides a single government cloud strategy.

"I would say in the market today, you see a lot of fragmentation, a lot of one-off solutions, people treating infrastructure-as-a-service different from software-as-a-service, different from platform-as-a-service," Niehaus said. "And, what's uniquely valuable about Microsoft is that we are building government cloud solutions that span all of that, from infrastructure to platform, to software. We think about it as infrastructure, productivity and business applications - a single portfolio of those government cloud solutions. What we're doing that's most valuable to customers is providing one single government cloud strategy."

Paramount to Niehaus and Microsoft, he said, is providing a seamless platform. "The key thing for my team," he said, "is to orchestrate how we ensure that all of those pieces are brought together into a cohesive platform, so that when we talk to our customers, we really offer that full broad suite of government cloud solutions, unlike any of the other providers in the market."

Niehaus added, "We think of government holistically and we think of each mission that government has, whether it's Health and Human Services for HIPAA or financial and

revenue and tax management, such as IRS 1075, or criminal justice and public safety. We continue to invest in achieving compliance with the regulations and standards our government customers require for each of our online services within our government cloud solution."

In addition to the single government strategy and roadmap, Niehaus said that government users of Microsoft's cloud services can expect a better total cost of ownership of existing infrastructure.

"When people look for a path to move to the cloud, the number one concern they should have is, will that cloud roadmap offer me lower cost of ownership with my existing IT investments, and a better ROI?" Niehaus said.

Niehaus noted that many of the services Microsoft builds in the cloud can also be deployed on local systems.

"Many government agencies have made investments around Microsoft Exchange, SharePoint and Active Directory and those are the same tools that are running in the cloud," Niehaus said. "So we make sure that they have both a clear roadmap for running that hybrid scenario, and that combination of on premise and cloud solutions."

"We want you to have cloud on your terms. We want you to be able to build the cloud IT infrastructure that best satisfies the mission requirements of each and every government agency," said Niehaus. "We strive every day to make government more efficient, both in their spending and in their ability to meet mission requirements- and we're delivering."





# The ABCs of XaaS

North Carolina's strategy to create a cohesive IT network

In November 2013, North Carolina Governor Pat McCrory issued "Executive Order 30," which mandated that state agencies begin "collaborating as one IT." The genesis was IT excess, said Chris Estes, state chief information officer.

"We had too many silos, too many systems and too much duplication," Estes said. "Each of the agencies was run as autonomous businesses. The governor...wanted us to work as a team and start breaking down those silos."

The task of updating and streamlining the state's IT infrastructure fell to Estes and the Office of Information Technology Services (ITS). To create a collaborative IT environment, they created an "ABC strategy" that outlined three goals for North Carolina's optimal technology infrastructure.

An ongoing challenge is maintaining communication around this strategy and its implementation, Estes said. To make sure the strategy is consistently applied, he and ITS use traditional communications such as newsletters, e-mail, and website promotion. However, the primary medium is face-to-face collaboration.

"I meet with agency CIOs," he said. "I meet with the governor and the Cabinet. Every week we're in these meetings talking about things that affect the citizens of North Carolina and we apply these principles to them."

Three "ABC" goals consistently guide decisions to transform North Carolina's IT into a virtualized, cohesive environment. They are:

## Accelerating customer centricity

"The first thing that we need to do is think about how the consumer interacts with technology, whether that be a state employee working on behalf of an agency or whether that be the citizens themselves," Estes said. Therefore, when considering new solutions, agencies look at all the potential stakeholders in that technology.

Several consumer-oriented ideals pervade decision processes, he said. For instance, "we want our users to be able to use any device, anytime, anywhere," he said. "So as we make business decisions for IT, we want to enable that." IT managers are also encouraged to "digitize to modernize," meaning new solutions should allow the organization to make as much information digital as possible so that state resources are accessible to the greatest number of consumers.

## Balancing risk

Even as agencies strive to accelerate modernization, Estes and his team ensure that each step forward is made with appropriate caution and consideration.

As part of this strategy component, North Carolina maintains a "try before you buy" standard of procurement. The heart of this process lies with the Innovation Center (iCenter), a state-funded environment that lets users test technology before investing in it. "The combination of knowing what we want, with solid business requirements, and then testing it to make sure it does what it's supposed to do should allow us to deliver more projects on time and on budget," Estes said.

So far, North Carolina has transitioned to Microsoft Office 365 and created a hosted virtual desktop in order to streamline agencies. The iCenter tested both solutions before they were deployed to make sure they could seamlessly integrate with the existing state IT infrastructure.

## Collaborating as one IT organization

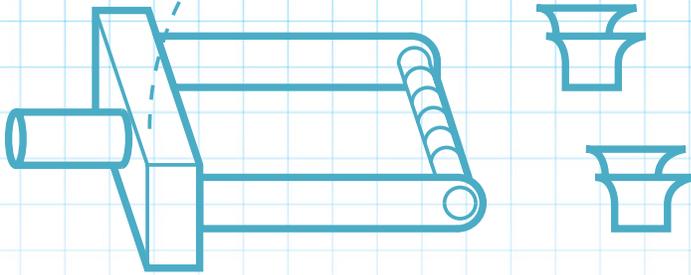
Estes and ITS want new technologies to foster collaboration among disparate IT organizations. This strategy component guides their decisions to train employees and choose technologies.

First, Estes is focused on cultivating IT talent so that all technology professionals have the skills to appropriately use new solutions. This will also help IT professionals collaborate across organizations.

At the same time, "IT needs to transform to work as a team, not only with our people. Our technology has to be built to work together," Estes said. Therefore, it is required that any newly deployed platforms communicate with all other technologies across state organizations. This ties directly back the "A" component by allowing consumers to work across platforms.

Together, these three principles drive cloud procurement decisions in North Carolina. Estes said the ABC strategy will "make government more efficient, easier to do business with and improve citizen interactions." By constantly focusing on this strategy, North Carolina's IT organization can move in a positive, cohesive direction.

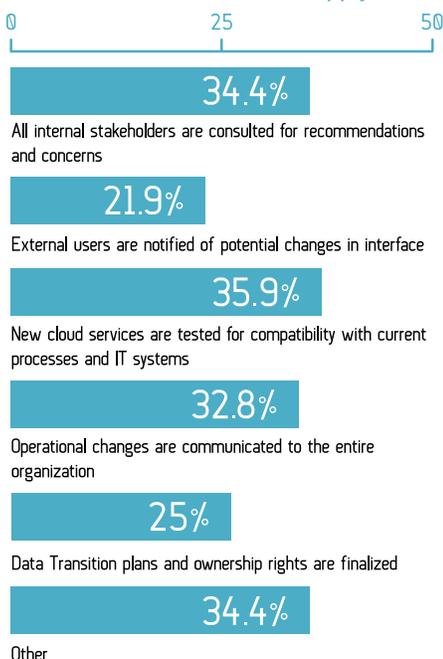
# Executing XaaS Strategies



**There is no set one-size-fits-all** approach to executing a cloud strategy. Some organizations may want to begin by transitioning easily replaceable services, such as e-mail. By targeting easy transitions, you can build confidence in the cloud process — and see where your strategy needs improvement — before committing to more resource-intensive cloud transformations.

Alternatively, some organizations may want to start by building a cloud architecture in which smaller solutions can be integrated down the line. This approach is more resource-intensive upfront, but it may yield greater immediate benefits and make the transition to cloud easier to streamline in the long term.

**When acquiring new cloud services, what steps does your organization take before deployment to ensure that transition is smooth and effective? (check all that apply)**



Once you have a XaaS strategy in place, carry it through to each cloud transition. Wherever you start your cloud journey, key factors must be incorporated into your acquisition, testing, and deployment processes. We detail them below.

**Time.** One reason government is adopting a XaaS mentality is that it allows agencies to keep up with the quick innovations of the private sector. However, that speed has a downside. It shortens the time required to test, integrate, and deploy solutions, thereby making it easier to implement a cloud service without due consideration. The speed of cloud implementation must be weighed against the need to scrutinize a solution's functionality and appropriateness for the current IT infrastructure.

**System readiness.** This recommendation comes directly from the Federal Risk and Authorization Management Program (FedRAMP), a governmentwide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. Before transitioning a service to the cloud, make sure it makes sense to replace your local system. If the solution in place is cost effective and meets business needs, it may not need replacing. What's more, severing an existing service contract may cost more than you'd save by using a cloud solution. Systems that are at the end of their lifecycle, either contractually or operationally, are better candidates for transition.

**Stakeholder input.** Your IT workers may be making the ultimate purchasing and deployment decisions, but more often than not, they are not the employees who will actually use new cloud solutions. Before drafting a cloud strategy, and especially before implementing specific cloud initiatives, it is imperative that all stakeholders get a chance to express their needs, concerns, and guidance.

These stakeholders will also have a better understanding of how a new system will interact with or interrupt their current processes. "Involving your security, privacy, records management, finance, program management, eDiscovery and other applicable parties from the beginning of the process will ensure an informed, complete development," according to FedRAMP.

**Communication.** We asked our GovLoop audience for tips to implement cloud services more effectively. One respondent said, "Simply tell everyone, and make sure that numerous demonstrations and examples are provided." It's a simple suggestion, but also a very important one. Communicating individual transitions to cloud services is just as vital as making your overarching strategy known.

Without advance notice and understanding, the likelihood that a new solution will be used inappropriately or inefficiently is high. What's more, communication facilitates feedback from users, which can be used to increase the efficacy of your cloud solutions. Finally, this tactic can increase buy-in from your employees.

"Some IT staff feel insecure about their job [when cloud solutions are deployed]," a respondent said.

Communicating the logic and strategy behind cloud transitions can mitigate concerns and increase support for the new solution.

**Training.** Training your internal users on new cloud services serves two purposes. First, it allows employees to become acquainted with a new solution before it is deployed. This will ease transition pains, and ensure they use the new solution properly. Second, this training provides another avenue for them to offer feedback.



# Digitally Powered Government: The Way Forward



## Rapid App Development in the Cloud

Your agency is under pressure to deliver innovative applications that accelerate mission attainment and improve service delivery – while reducing costs. Appian's enterprise application platform unites business processes, enterprise data, mobile access and social collaboration – on premise or in the cloud. As the market leader in modern Business Process Management (BPM) platforms, Appian delivers accurate, quality data from systems of record to knowledge workers (in the office, or on-the-go), and provides the foundation for adaptive case management, effective business processes and enterprise collaboration. The result is smarter decisions, faster actions, and holistic visibility into the overall health of your agency.

# Appian

# Using Cloud Today... and Tomorrow

An interview with Chris O'Connell, Vice President of Federal at Appian

Today, most public sector organizations have begun their cloud journey. But fewer agencies are thinking ahead to consider what the next disruptive technology will be. We sat down with Chris O'Connell from Appian, a business process management application platform provider, to learn how new cloud adopters can simultaneously meet the technology needs of today, while preparing for the potential changes of tomorrow.

"The economic value of cloud computing is hard to over-state," said O'Connell. "It's now proven that cloud platforms can be at least as secure as on-premise installations. But cloud computing is not a panacea and, if not approached carefully, can lead to many of the same issues that afflict traditional systems. It comes down to flexibility and ownership."

Cloud adopters must avoid platform lock-in. A modern platform should work in any cloud environment without changes to the underlying software. Otherwise, you're locking yourself into the environment, without the agility or scalability that agencies need. Agencies must also retain ownership of their data, application logic, and interface design.

The ability to transition between public cloud, private cloud, and on-premise without reconfiguring applications is essential. Platform-as-a-service and software-as-a-service can still lock you in if you're going down the traditional path of software that only allows you to do certain things. If your mission changes because of legislation, policy, or reporting needs, your cloud platform must grow with you to deploy changes rapidly.

Appian believes a platform should be able to transition from the cloud if necessary. Cloud reduces traditional IT burdens, but what agencies need most of all is flexibility to adapt and change. There may be times when

you need to pull a cloud system on-premise, temporarily or permanently.

"Appian Cloud is unique in that once you have deployed it, you can pull it in-house if you need to. It's a simple matter of exporting an application package from one environment to another. This flexibility helps agencies serve the public better," said O'Connell. "Agencies hamstrung by rigid systems are unable to meet their core objectives. We give agencies the freedom to innovate within a flexible, secure environment."

Commercial companies differentiate in the marketplace based on how quickly they respond to customer demands. Government has the same requirement. Appian helps agencies prepare for change through agile software that can adapt to any IT environment.

One example O'Connell offered was the Integrated Defense Enterprise Acquisition System (IDEAS) application currently deployed at the Defense Information Systems Agency (DISA) within the DoD. He explained, "This Standard Procurement System replacement is sitting in the DoD cloud, accessible by mobile devices, and is providing service to multiple agencies across the DoD. Federal acquisition work requires the ability to go back and show exactly what was done, what decisions were made, and why. System architecture changes over time do not affect our ability to maintain those records and provide that audit trail."

Speed of delivery is also a benefit for Appian customers. A cloud environment can be up and running in minutes. "Appian is rooted in a model-driven, visual development approach – as opposed to traditional coding – so new, innovative business applications can be configured and deployed in a fraction of the time it used to take," said O'Connell.

That highlights another immense point of value: modernization and innovation. "We mask complexity so our customers can focus on turning things like mobility and social collaboration into immediate value," said O'Connell. "For example, Appian delivers mobile for free. Any Appian application is immediately available on the desktop and mobile devices without additional coding." Because software reconfiguration no longer has to take place with each change in the IT infrastructure, agencies are able to dedicate more time to their core missions.

O'Connell also said agencies need to think in new ways about how software can accelerate smarter decisions and faster actions: "It's about the marriage of data and process, delivered in an intuitive and action-oriented interface. Today's government knowledge workers spend way too much time searching across different systems for the right data, digging through broken stovepipe applications to compiling the data they need. Then, they execute decisions in another set of applications, maybe something structured and somewhat auditable, but often simply via email."

"We provide a single and consistent user experience across any device, across any set of enterprise data, across any business process," said O'Connell. "There's a mindset change that goes along with this, and agency employees on both the business and IT sides need to adjust to it. Once they do, they realize Appian is an application platform for managing the complexity, size and scale of the federal government via applications that are simple, intuitive, deployable, and accessible."





# Cisco, Enabling a World of Many Clouds

Government IT organizations are facing a new set of challenges, as the consumption of IT is shifting from the traditional model of acquiring hardware and software and deploying it onsite, to a managed or cloud services model.

Applications, content, and services are now being delivered through the cloud.

Cisco is helping public sector organizations architect and use technology to take advantage of both commoditized and enterprise IT.

**To learn more about how Cisco can help manage these changes in IT consumption, visit [Cisco.com/go/fed](http://Cisco.com/go/fed) and [Cisco.com/go/govcloud](http://Cisco.com/go/govcloud).**



# Traps to Avoid When Implementing Cloud

An interview with Mike Younkens, Director of US Federal Systems Engineering at Cisco

Across government, agencies are implementing and utilizing cloud infrastructures that efficiently and effectively deliver services to citizens and transform the business of government. Although cloud is becoming the norm, implementation can still be tricky -- and there are pitfalls to avoid when choosing and deploying a cloud service.

To help government users avoid these cloud traps, GovLoop recently spoke with Mike Younkens at Cisco, who gave us a variety of tips to help make better decisions around cloud technology.

"I think that cloud services in general are extremely attractive, because they give you the opportunity to get working on whatever task you have that you want to work on," said Younkens. "You can work on it right away. But there's some traps in cloud that I think people have to figure out right up front."

Younkens recommended that potential cloud adoptees consider costs, capabilities, and fit into an overarching strategy before committing to any single solution.

"First of all," said Younkens, "I would encourage people to really understand what the total cost of the activity that they're going to consume is. Meaning, what does it cost to get started? What does it cost to consume services? And then, the tricky one, what does it cost to move back out of that when your work is done, or you want to move your work to a different location, what costs are involved in getting that part of it done?"

Younkens' second important consideration

to follow is what he refers to as the cloud onboarding process. "One of the other things that I found that really distinguishes the difference between cloud providers is their onboarding process," he explained.

"If you're a government agency and you're trying to solve very specific sets of problems and you're looking at cloud as a way to go get the service to solve that problem, you really want to understand the cloud service provider's capability, and whether their capabilities align with the problem set that you're trying to solve," he added. "Is the cloud provider you're looking at set up to provide that type of service? Do they have good onboarding that will let you bring the data in? Do they have good analytical tools available to you to solve certain problems?"

For Younkens, though, the easiest cloud trap to fall into -- and potentially the most deadly -- is the one of not planning your cloud needs and strategy ahead of procurement and implementation.

"It's the classic trap of not planning anything," Younkens said. "You don't understand the totality of the cost that you're dealing with. And to me, that is the real trap."

Younkens elaborated that the impromptu nature of cloud services and pay as you go billing can be deceptively simple. He explained that pay as you go cloud services can be great for, say, start-up businesses, because if you're building something, you only need to be using as much as your growing business requires. But it's very different for government agencies.

"Well-established government agencies aren't necessarily just trying to launch a new business," Younkens said. "They're actually trying to solve a mission problem. It's so easy and attractive to go and consume compute services, but it just grows and grows and grows, and eventually it can get out of hand. So if you don't have a good strategic plan to understand how you're going to take advantage of those services, and then some rough order magnitude of what it's going to cost, you can end up getting yourself in a pretty ugly budget bind."

For those hoping to avoid these pitfalls in cloud implementation, Cisco offers consulting as well as cloud services to make sure their customers are making the best choices possible.

"Our consulting services can help customers understand these concepts that we're talking about," Younkens said. "If they're trying to make a strategy to decide what they want to keep on premises, what they want to move in the cloud, how are they going to operate in the hybrid cloud environment -- we offer services to help get that done."

"We have a tremendous amount of value to add in the cloud conversation, based on our years of experience and based on our innovation," Younkens added. "So I think that from a services perspective, what we could offer is we see this as a journey with our customers, a journey to the open hybrid cloud, that's going to take some building blocks to get there. And we're there to help."



# XaaS is Not Always Cloud-First

Georgia's strategy to leverage cloud when appropriate

**XaaS is a cloud term.** Therefore, it's not surprising that many IT managers equate XaaS strategies with cloud-first strategies. However, in order to use everything-as-a-service in a way that doesn't disrupt current processes or complicate IT infrastructures, many organizations develop cloud-when-appropriate strategies. This latter option is what Calvin Rhodes, chief information officer, and Steve Nichols, chief technology officer, at the Georgia Technology Authority (GTA) use to drive technology decisions in their state.

Georgia's IT infrastructure has been built to leverage an economy of scale. Rather than contracting with external cloud providers, GTA has its own North Atlanta Data Center, which it uses to provide many shared services to state and even local government organizations on a pay-per-use basis.

To continue exercising this model, GTA

requests that administrators first consider using the state's existing IT infrastructure for technology transitions, rather than turning to external cloud providers. This preference is outlined in its [Enterprise Operational Environment](#) standard. If a state agency wishes to pursue a cloud option for production, it first has to file an exception with the state and make a case for why its solution would benefit most from a cloud service. However, test and development for low impact systems do not require a waiver as defined in its [Cloud Services Standard](#).

In some cases, Rhodes and Nichols agree that cloud is the best option. For instance, the state's web presence relies on cloud technology. "There weren't security concerns or regulatory concerns because it's all public information anyway," Nichols said.

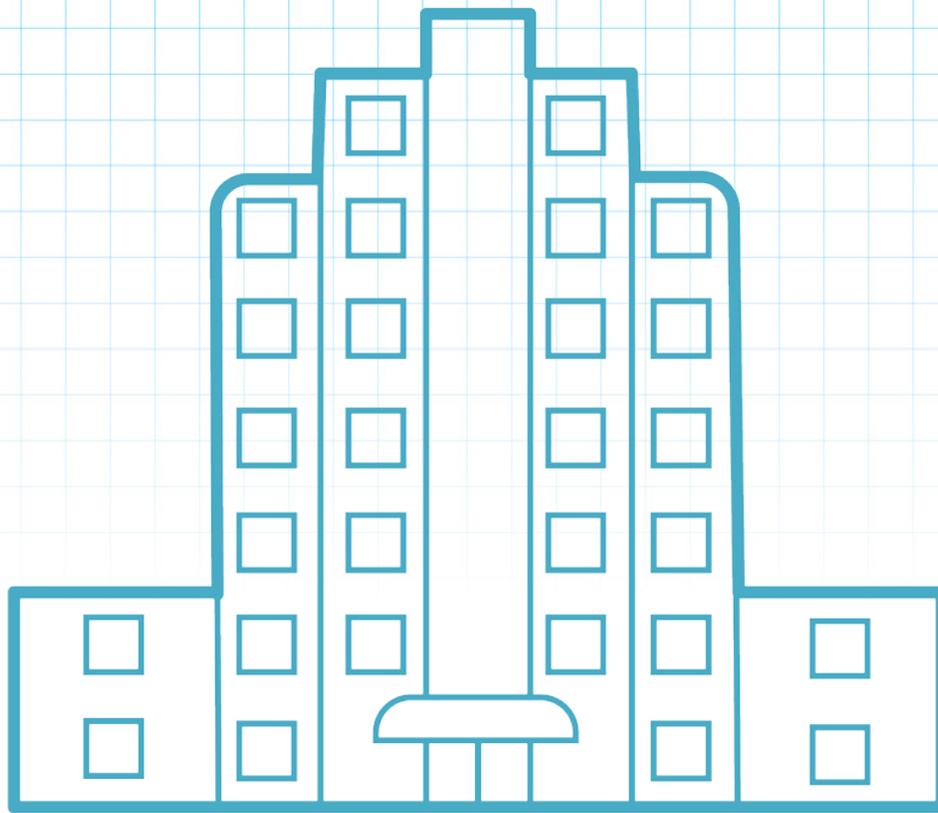
Now, Georgia.gov and multiple agency websites rely on the free Drupal content

management system and are hosted in a public cloud.

Rhodes offered another example. Six of Georgia's agencies run their own contact centers. Recently, the system that ran these contact centers reached its end of life, and building a new local system would have been costly. "Because technology is changing so rapidly, it was much better to do a multi-award cloud contract providing agencies several choices," Rhodes said.

This approach also offered each agency the ability to contract for a solution that would meet its individual business needs. Despite GTA's preference for state enterprise solutions, "that doesn't mean that if someone has a unique need that doesn't fit, they can go through the process for a waiver," Rhodes said.

When a waiver is granted, GTA still ensures that the cloud deployment process



integrates with the state architecture and safeguards the agency. “If an agency is considering a software-as-a-service solution, we’re going to show up and say, ‘OK, but there’s some key things you need to be concerned about,’” Rhodes said. He added that security provisions and data ownership are primary considerations.

Nichols also emphasized the need to create an off-boarding plan before a cloud solution is acquired. “Governments aren’t geared up to think that way — of having to scramble and vacate a system in 30 days,” he said. “So that’s the thing I spend the most time talking with agencies about. You have to understand that when you joined this very agile world of cloud, that that knife cuts both ways. They can get you up and running very fast, but they can also be gone in a heartbeat.”

Agencies can adopt cloud solutions when necessary, but sometimes the current IT

architecture makes cloud transition a less preferable option. Nichols cited the state’s new Medicaid eligibility system as an example. Although agency officials originally wanted to pursue cloud options, a request for proposals set out terms that weren’t conducive to reaping the benefits of cloud. To remain compliant with regulatory requirements and prevent disruption of current processes, a new provider would have had to reformat its operations to integrate with existing local document methods, imaging systems and data center components. That level of customization would have diminished the advantages of using a cloud provider.

Rhodes also said regulatory adherence is particularly difficult for states because they have to meet both federal and individual state mandates, which can change frequently.

Nichols agreed: “The first litmus test is if [the

cloud provider] has any of these specialized regulatory requirements which you wouldn’t normally find in a commercial offering.”

However, the driving consideration for adoption of new technologies is the ability to integrate with and simplify Georgia’s IT enterprise. In some instances, a cloud solution may be used to fulfill particular agency needs. However, in other instances, they may disrupt Georgia’s IT economy of scale. “As we start designating systems as enterprise, we are just looking forward from this point to try to start moving the agencies in a common direction,” Rhodes said.

This vision of linking all states agencies together under a cohesive, pay-per-use IT architecture is what GTA describes as using “technology as a service”. This is a XaaS strategy, but it is not a cloud-first strategy.



# Hitachi Unified Compute Platform (UCP)

Where efficiency and reliability **converge**

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

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

[www.hds.com](http://www.hds.com)

# Easing the Transition to XaaS

## An interview with Darren House, Director of Solution Management at Avnet Government Solutions

Cloud is now the aggregation and incubation point for organizations to change business models and work more effectively. Despite the efficiencies cloud solutions can offer, the transition of services to this innovative new environment can be taxing on an organization.

To discuss how government agencies can ease the cloud transition, we spoke with Darren House from Avnet Government Solutions, a value-added solutions distributor focused on government markets. House emphasized that agencies should be selective in the services they transition to the cloud. “The cloud is really just one tool in the toolbox,” he explained. “It’s not a cure-all solution, but an enabler for optimization, efficiencies and transformation. It’s a means to an end. It’s not an end in itself.”

To determine where cloud could be an appropriate solution, agencies have to examine the needs of their mission. House said, “It’s an opportunity for an agency to strategically examine what its core mission is and the core skillset needed to achieve that mission, so a long-term plan to transition support services best-suited to a cloud service model can be determined.”

Ultimately, the agency must decide which services are core versus ancillary. But Avnet Government Solutions’ unique expertise can offer valuable guidance. “We have identified the main areas that are a natural for government agencies to transition into the cloud, outside of their core expertise. We have invested time and resources into developing these offerings. When our partners bring these solutions to government agencies, they are able help them more cost-effectively address their ancillary service needs, freeing the customer’s IT team to focus on their

core mission,” said House. “One example is Hitachi Data Systems (HDS) Federal’s Cloud Services for Content Archiving, which provides enterprise data archiving capabilities at a lower cost than most organizations can provide for themselves.”

Moreover, a solutions distributor like Avnet Government Solutions can help value-added resellers (VARs) match cloud solutions to identified customer needs. “It’s really about categorizing and prioritizing the different areas of the service offerings in the market, and identifying which ones provide the clearest value to the organization,” House said.

This value is often determined by challenges facing government agencies. “We focus our enablement around the needs within the market. For example, the government is looking for Common Off The Shelf (COTS) solutions, integrated with some hyperscale/cloud elements tailored to government enterprise consumers. HDS Federal’s Hitachi Content Platform (HCP) Anywhere file synchronization solution provides the capabilities and features of DropBox or Google Docs, but tailored for the enterprise government customers,” said House.

Avnet Government Solutions links these challenges to the most optimal cloud solutions. House explained, “We have teams that know the technologies and how to get them implemented to support these needs. For example, we’re experts in the converged and hyperconverged markets that are emerging as the baseline infrastructure for the hybrid cloud architecture. HDS Federal’s Unified Compute Platform (UCP) and the recent announcement of their involvement with VMware’s EVO:RAILS in the hyperconverged market are the solutions government

customers need to move data center consolidation, application rationalization, cloud-first efforts forward in order to grease the skids for XaaS.”

And while these packaged solutions are multi-faceted, Avnet Government Solutions ensures they will not add complexity to your agency. “We prebuild converged infrastructures, like HDS Federal UCP, for the VARs within our solutions center, and have it ship out to the government customer’s site, ready to go,” said House. “Avnet’s VAR partner can immediately start the application configuration and integration within the environment, reducing costs, complexity, risk and time-to-mission value.”

“Most agencies are going to have a hybrid cloud model,” House added. “They’re going to have some traditional IT, they’re going to have some private cloud, and they’re going to have some public cloud. The big part is how you manage and maintain these various solutions. By understanding the market need, the technologies that deliver on that need, and the VAR expertise in delivering and integrating solutions, Avnet Government Solutions is at the nexus of the move toward implementing technologies that will drive XaaS evolution.”

Ultimately, government organizations will have to dedicate time and resources to creating an effective XaaS infrastructure. However, the effort required to transition to the cloud can be drastically minimized by partnering with a value-added solutions distributor to identify areas of opportunity, increase your knowledge-base, and reduce the complexity of your cloud environment.



# The Impact of XaaS on Procurement Processes

**Purchasing cloud services** requires a procurement process that is quicker and more agile than traditional pathways, but also one that is more conscious of the implications of purchasing offsite services. Considerations such as data ownership, implementation speed, transition of systems, and offsite information security are crucial components of cloud procurement processes.

What's more, these new procurement guidelines should be deployed across all departments and teams. "Have an agency-wide approach to purchasing and implementing cloud services," a survey respondent said, because this ensures that systems remain compatible with other internal systems, your organization's regulatory environment, and your overarching XaaS strategy.

Procurement practices will vary depending on the cloud solution that you are acquiring. For a detailed analysis of procurement considerations for IaaS, SaaS, and PaaS purchases, we recommend referencing The Center for Digital Government's *Best Practice Guide for Cloud and as-a-Service Procurements*.

However, there are overarching themes that should be applied to any cloud procurement process. Those themes are:

## Updates and maintenance

A primary benefit of cloud solutions is the ability to update entire systems in real time, with little notification or effort from your IT department. This has important implications for your procurement process, because the solution you acquire may not look the same, act the same, or meet the same regulatory requirements in the future. Therefore, as you procure new cloud solutions, guidelines for these updates and maintenance must be firmly outlined.

One of our respondents said their team constantly checks with its IT and legal teams to guarantee they remain compliant. "We consult with our IT department to ensure our data is backed up and stored properly for public record purposes while we also consult with our legal team to ensure we are maintaining proper recordkeeping strategies," the respondent said.

However, the burden of ensuring systems remain in compliance should not be placed solely on your organization. Well before a system is put in place, language should be included in contracts and protocols should be developed to ensure that any updates by a cloud service provider will be discussed within your organization before deployment. Similarly, the cloud service provider should commit to keeping updates consistent with current regulatory standards.

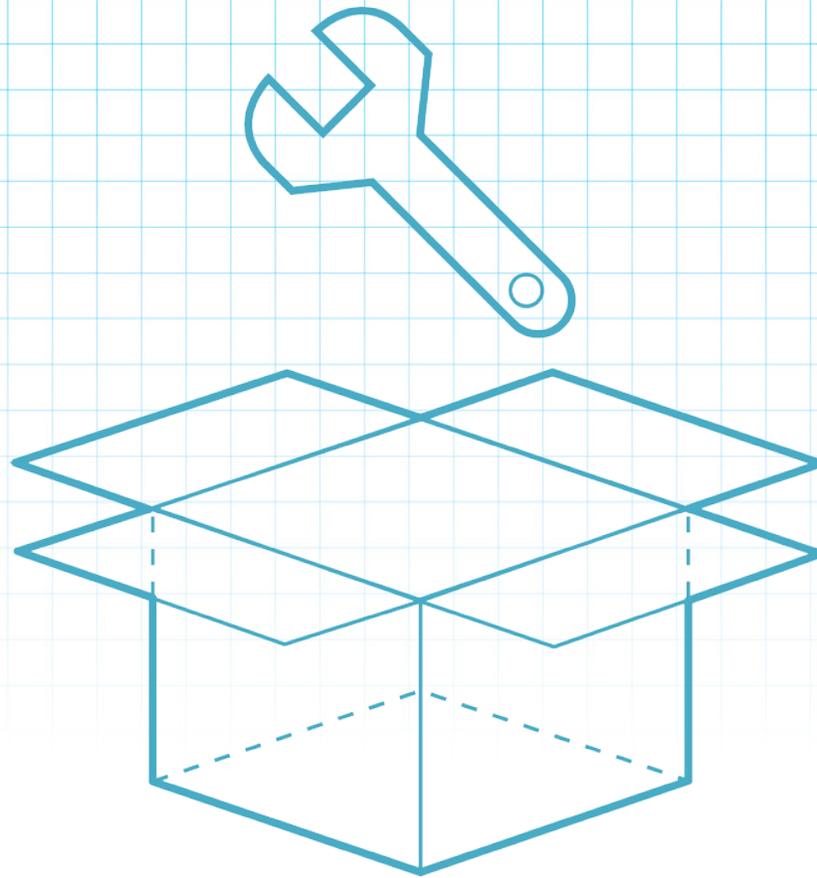
## Responsibility for technology

When you build on-premise IT systems, the costs for equipment and upkeep are obvious. Your organization owns the technology and therefore must pay for its maintenance. However, different cloud models will have different terms of responsibility for the technology. For instance, a SaaS provider is responsible for the technology stack and has more responsibility for protecting data. Conversely, an IaaS service provider has less responsibility, because it essentially leases its technology to you for upkeep and use. Whatever the solution, your procurement process should strictly delineate which parties have financial and operational responsibility for which parts of a cloud solution.

## Security

With cloud solutions, you must not only locally safeguard your data, but also make sure each cloud service provider has the appropriate security measures in place to protect the confidentiality and integrity of your data. For instance, you must now consider whether a service provider will encrypt sensitive information and relegate who has access to your data within their own organization.

As part of FedRAMP, NIST issued *Guidelines on Security and Privacy in Public Cloud Computing* to help organizations analyze



the threats, technology risk and safeguards that surround cloud offerings. They detail nine areas of security concern: governance, compliance, trust, architecture, identity and access management, software isolation, data protection, availability, and incident response. For each security issue, recommendations for service provider scrutiny are offered. Ensure these considerations drive your procurement and contracting decisions.

## Regulatory requirements

As with any IT project, new technology must meet certain regulatory requirements, such as the Freedom of Information Act (FOIA), eDiscovery and Section 508 of the Rehabilitation Act. However, your procurement process will need to address additional regulatory constraints, such as provider residence in the continental United States, if the technology in question is cloud-based.

FedRAMP offers certification to cloud service providers proven to be “FedRAMP Ready.” Additionally, the program suggests consulting other agencies or government organizations to see what cloud solutions they have effectively deployed according to regulations. The program even provides a [webpage of success stories](#) that details solutions acquired by agencies including the

Defense and Energy departments and the U.S. Securities and Exchange Commission.

If you choose a new cloud solution, use rigorous testing and explicit contract language to ensure the service provider will consistently meet your agency’s regulations. Even as cloud providers take your data offsite, ultimate responsibility to control your information remains with the agency.

## Data ownership

This is the biggest distinction of cloud procurement concerns. With local systems, any data stored there clearly belongs to the organization. As data transitions to private, public and hybrid clouds, data ownership and rights become less obvious.

In XaaS contracts, data ownership is usually a shared responsibility between your organization and the cloud provider. This means that the same ownership rights and responsibilities that your organization uses may be relegated to the cloud service provider. Clear distinctions should be made between your organization’s roles and responsibilities and those of the provider. Moreover, any data rights given to the provider should be well defined so that your data is being accessed and used only when necessary.

## Exit strategy

Just as it’s easy to quickly deploy a cloud solution, it takes very little to sever a cloud service. A GovLoop survey respondent asserted, “Agencies must have identified any migration costs to roll into a cloud service and must have a planned exit strategy, understand migration costs to roll off of a system, and test that plan” before solutions are acquired. Your procurement strategy must not only consider the transition to a cloud service, but also how ownership rights, technology costs, and information storage will change if that cloud service is abandoned.

This also relates to our previous consideration of data ownership. Before contracting with a cloud provider, a detailed understanding of what would happen to your data at the end of an agreement should be in place. Many public sector organizations are required to safeguard records indefinitely. Therefore, their cloud contract should ensure that no data will be lost, or remain with the cloud provider, if the service is severed. This is commonly covered in a “migration at termination” clause, which requires the cloud provider to transition any data back to the agency before deleting it from remote servers.



# Planning Guide

## Questions to ask:

Before committing to a new cloud solution, methodically answer each of these questions so you can be sure the technology fits with your current infrastructure, ongoing processes and long-term IT goals.

- ▶ How does this solution fit into our overarching XaaS strategy?
- ▶ What other processes will this system affect?
- ▶ Who will use this new system?
- ▶ What business or technical needs will this new service address?
- ▶ Will it create any new business or technical needs?
- ▶ Will users be able to navigate it easily, or will training be required?
- ▶ How will this solution interact with local systems?

## Stakeholders to consider:

Before, during, and after deployment, ensure every person who will interface with a new cloud solution is solicited for feedback about how the transition will affect their current processes and other IT systems.

- ▶ Internal end users
- ▶ IT personnel who will deploy and manage the service
- ▶ Other agencies and organizations that will interface with the new technology or process
- ▶ Internal departments who must interact with the system or its outputs
- ▶ Public users who will see or use the service
- ▶ Finance department
- ▶ Security team
- ▶ Information management personnel

## Local vs. Cloud Service Provider (CSP) concerns to address:

Procurement Aspects	Local Technology	Cloud Technology
Updates and Maintenance	Deployed by on-site IT team, often after detailed scheduling and planning	Executed automatically, without advance notice to IT or regulatory team
Responsibility for Technology	Responsibility lies with organization exclusively	Dependent on cloud model deployed, but responsibility most often shared with CSP
Security	Security relegated to on-site observers	Must be regulated across off-site CSP and on-site IT operations
Regulatory Requirements	Standard information technology regulations (FOIA, eDiscovery, 508) apply	Additional requirements, including off-site security, FedRAMP ready certification, and residence in CONUS, to be considered
Data Ownership	Ownership and responsibility for security lie solely with government organization	Ownership and responsibility are shared with CSP
Exit Strategy-	straight-forward with minimal concern for data migration or loss at predetermined end of contract	Unclear, as service agreements can be terminated without notification to CSP or preplanned migration of data

## 10 Steps to Deployment:

Regardless of the cloud solution being deployed or process being revamped, follow these ten steps to ensure your transition to cloud services is executed without complicating your IT infrastructure or disrupting current processes.

1. Identify needs to be met by a cloud solution.
2. Solicit stakeholder feedback on concerns and suggestions for cloud options.
3. Test possible cloud solutions within your current architecture.
4. Compare solutions to the regulatory environment and risk tolerance level of your organization.
5. Choose a solution and develop a plan to integrate cloud service into the existing IT architecture.
6. Communicate decisions to the entire organization and external stakeholders.
7. Train employees to use the new solution and incorporate it into current work processes.
8. Deploy the cloud solution.
9. Test and again ask for feedback from all stakeholders.
10. Optimize cloud service integration with existing infrastructure.

# About Govloop

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Hannah Moss, Research Analyst, GovLoop, at [hannah@govloop.com](mailto:hannah@govloop.com).

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

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

**Twitter:** @GovLoop

[www.govloop.com](http://www.govloop.com)

# Acknowledgments

**Our Sponsors:** Appian, Avnet Technology Solutions, Cisco Systems, DLT Solutions, Hitachi, Microsoft, Presidio, Red Hat, and ViON

**Author:** Hannah Moss, Research Analyst, GovLoop.

**Designers:** Jeff Ribeira, Senior Interactive Designer, Tommy Bowen, Junior Designer, and Jake Brennan, Design Fellow, GovLoop.





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