5 Questions You're Afraid to Ask About Cloud

BUT SHOULDN'T BE!

govloop

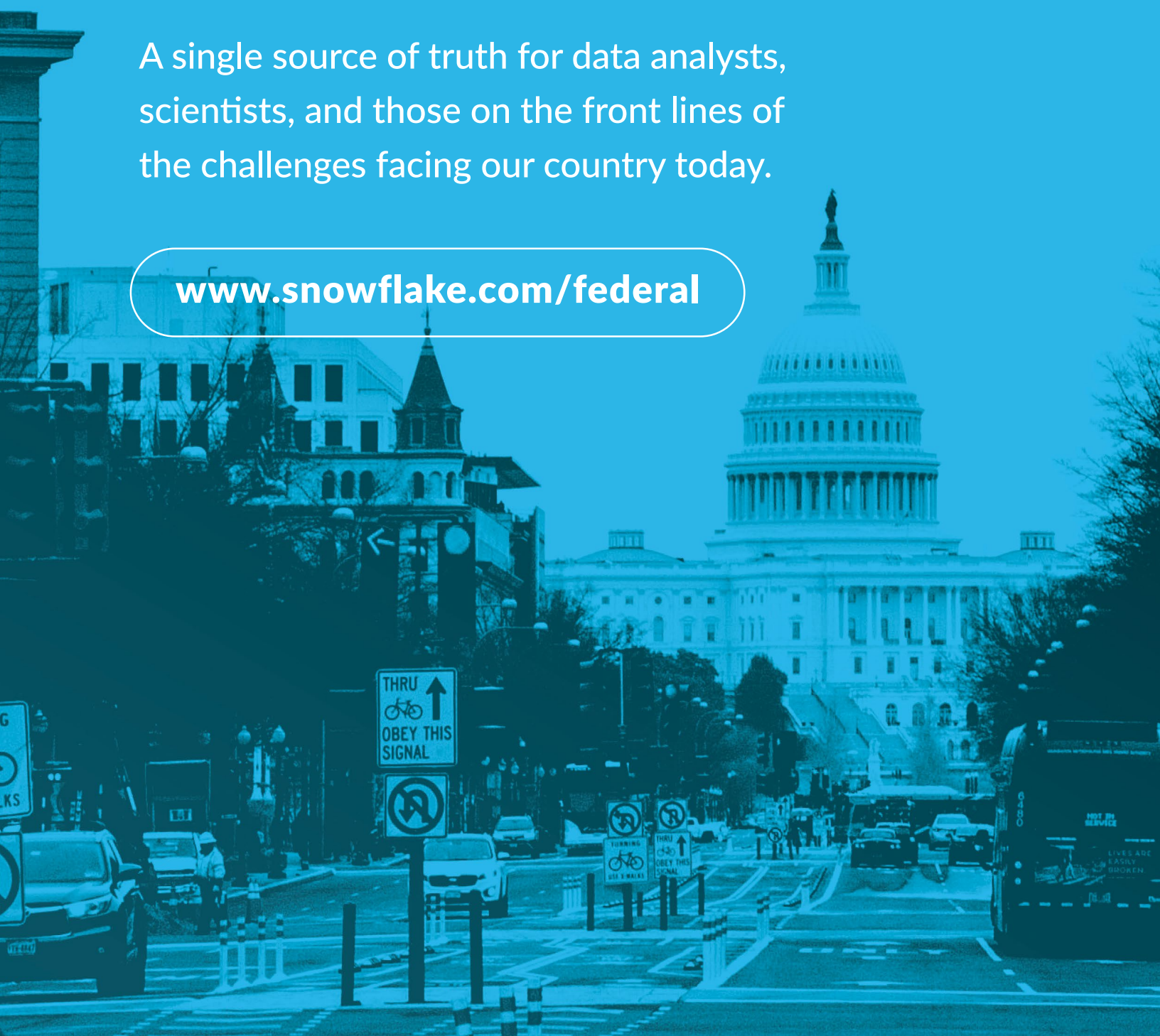
TABLE OF Contents

snowflake®

CLOUD DATA PLATFORM

A single source of truth for data analysts, scientists, and those on the front lines of the challenges facing our country today.

www.snowflake.com/federal



Executive Summary

Cloud is a tough topic to write about, but we know that even tougher is trying to keep up with all of the "extra, extra, read all about it" updates that dominate social media, news outlets and even Super Bowl commercials. Every year, new regulations come out, capabilities mature and a new as-a-service term is coined. But what does all of that actually mean?

For most government employees, very little changes as news cycles swirl around the famed technology. As cloud-based storage drives increasingly become the standard in our everyday lives, the overall government IT landscape is in relatively the same place it has been – lagging, disjointed and inefficient. Instead of boasting artificial intelligence (AI) and intuitive iPhone apps like the commercials promised, government employees are stuck with clunky in-house systems and USB drives.

Of course, some agencies can boast success stories. But for many, cloud is just something that tech departments call a game-changer; it doesn't actually deliver all that much revolution.

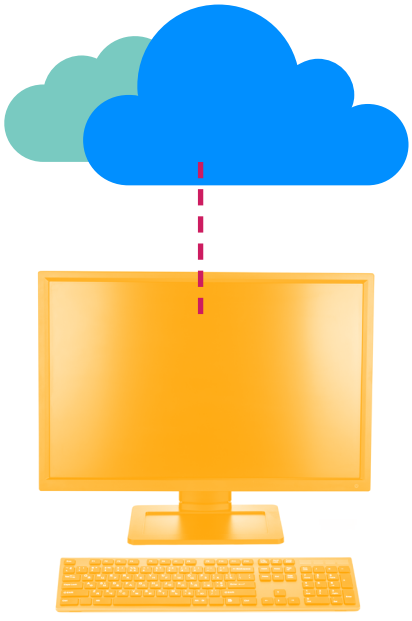
Consider this guide, "5 Questions You're Afraid to Ask About Cloud," a change-up. We don't want to tout cloud's potential without addressing the very valid concerns and questions that people have about the technology, starting from square one. Whether you're wondering about the security of your data in the cloud or the impact it will have on your day-to-day job, these sections have your answers.

1. **Do I need to learn new skills or systems to succeed in a cloud environment?**
2. **Does cloud really offer all the capabilities that advertisements promise?**
3. **Is cloud always worth it?**
4. **Is cloud safe for my data and me in the face of cyberthreats?**
5. **Will the cloud transform how I use technology in government?**

This resource was designed for you. The five questions that we address are based directly on what we've heard from community members throughout government. While some work in IT, security or acquisition, others are just interested users of the technology – program managers, accountants, analysts and the list goes on. And for as long as cloud has been around, its significance has only grown, as evidenced by the fresh relevance the coronavirus has placed on cloud-assisted remote work.

In the following pages, you'll read about what the cloud really is – not technical definitions or flashy supported services but its real impact. Far removed from the jargon and braggadocio, you'll find out what cloud can realistically do in government IT environments, what that means for your job and tips from experts.

To answer your questions, we spoke to Chris Chilbert, Chief Information Officer (CIO) at the Health and Human Services Department's Office of Inspector General (HHS-OIG), and Guy Cavallo, Deputy CIO of the Small Business Administration (SBA). Additionally, we studied reports from the National Association of State Chief Information Officers (NASCIO) and state and local organizations to see what best practices they had developed for cloud.



The Cloud Need to Know IN 2020

CLOUD 101

What even is the cloud?

Cloud computing is technological resources and capabilities that are delivered on demand outside of traditional on-premise solutions, usually through the internet or private shared networks. The cloud enables employees to collaborate on work from multiple locations or devices, as computing power transcends a physical server or desktop. Additionally, storage is generally taken out of the hands of individual agencies and instead placed with cloud service providers, which can then offer a variety of services to layer on top of existing data.

Cloud comes in a utility model called "as a service," in which you only pay for what you use. Just like you choose how often and how much to run the water at home, you do the same with cloud. And just like you have different areas for which you control the water, such as the bathtub, the garden hose or the kitchen sink, cloud can also be used for a variety of applications, infrastructures and features.

CLOUD STAGES

Crawl: Organizations are just getting started with or looking into cloud capabilities. They might migrate a small dataset as a pilot or primarily stick to cloud for email inboxes.

Walk: Organizations are investing in cloud for major projects and purposes. Employees are training on how to integrate and use cloud-based applications and services, and organizations have a clear mission with these technologies. Still, lots of data is kept on premises and legacy IT fails to synchronize with many of these new systems. Cloud is still not the overarching IT infrastructure.

Run: Organizations are all-in on cloud technologies. While there might still be the occasional need for on-premise systems, every new technology begins with the cloud in mind. Secure application development, communication and most user functions take place in the cloud, where data is centrally stored. Organizations use these capabilities to promote mobility, remote work and emerging technologies.

LEADERS IN GOVERNMENT

Health and Human Services Department Office of Inspector General

Small Business Administration

The Buzz Around the Government Cloud Community

TIC 3.0: By including cloud as an official use case, the newest update to the Trusted Internet Connections (TIC) initiative removed a regulatory cybersecurity barrier that previously had dissuaded many agencies from making the move. TIC was initially designed to limit the amount of external connections to federal networks, but as mobile devices, branch offices and remote work have expanded, TIC has grown to assure agencies that independently purchased cloud solutions will meet security thresholds. Additionally, the cloud use case bolsters the security leg of Cloud Smart, the Trump administration's effort to encourage and inform cloud adoption.

"Cloud is a lot more relevant in ways that it wasn't seven or eight years ago. It's just these alternatives that are available for agencies to consider. It's a huge leap forward in terms of federal IT cybersecurity, but again, it really is up to agencies for how they want to adopt [the new use case]."

– Sean Connelly, TIC Program Manager, Cybersecurity and Infrastructure Security Agency

JEDI: The Joint Enterprise Defense Infrastructure (JEDI) contract signified the government's strongest endorsement of cloud technology at its time of award. By choosing to go with one primary cloud provider to support an enterprise cloud, the Defense Department (DoD) contract would pave the way to "information superiority" and the ability to sync data with modern technology on the frontier of battle. The 10-year, $10 billion deal has hit several snags, but nonetheless makes clear a future state of government IT with cloud at the forefront.

"Cloud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage."

– Defense Department Cloud Strategy

Cloud Delivering Emerging Technologies: The as-a-service model lets agencies run application spin-ups that wouldn't have been possible with on-premise constraints. One example is how state and local governments have used voice response software, carried through popular Amazon Echo- and Google Home-enabled devices, to connect with constituents. The technology can field questions from what's required for driver's license exams to who the state's first governor was.

Are you cloud-ready?

The network enables the portability of applications and data between on-premises data centers and the cloud. The network connects everything – people, machines, and data, it is the “on-ramp” to the cloud.

LEARN MORE

www.cisco.com/go/cloudready

INDUSTRY SPOTLIGHT

The Steps to Enabling Agility With Networks

An interview with Grimt Habtemariam, Market Strategy Leader, Cisco U.S. Public Sector

When organizations are agile, they're able to respond quickly and effectively to business threats and opportunities. Who wouldn't want that?

Every organization seeks to be fluid in their market space. But while government agencies often operate quite differently from the private sector, they can follow the same industry best practices for adaptability and responsiveness.

"The goal for agencies is to enable digital business agility," said Grimt Habtemariam, Market Strategy Leader for Cisco's U.S. Public Sector. Cisco delivers data and network solutions that streamline government operations by connecting people, data, processes and things.

But as the saying goes, "nothing good comes easy," and agility is not some on/off switch. For government agencies to get there, they need to lay the groundwork.

GovLoop interviewed Habtemariam about what that looks like in the public sector and the steps agencies should take. Before becoming agile, agencies first need the data and network to support their enterprise.

1. Prioritize data and identify sources.

A few years ago, federal agencies were ordered to leverage data "as a strategic asset," and there have been tremendous gains since. The Federal Data Strategy now guides agencies' data governance and efforts, and state chief data officers have formed their own network.

These strategies and operational groups exist for good reason, but they're no substitute for what individual agencies must do at the ground level. Agencies need to use their own strategies and governance models to take stock of, standardize and plan out use cases for their data as more becomes available. Doing this up front will help to resolve privacy, confidentiality and security concerns.

"Agility cannot be achieved without data. And essentially data is the lifeblood of any organization's business agility," Habtemariam said.

2. Move to an intent-based network.

To capture and use data, organizations need a robust and comprehensive network for information to flow through. No matter where data is stored, for it to move efficiently, it must be transmitted through a network.

Hardware-centric legacy networks would limit visibility into the flow of data to physical boundaries. But new software-defined networks transform the operations and efficiency of networks with end-to-end data visibility across environments, and by leveraging built-in machine learning and analytics capabilities.

With modern intent-based networks, agencies can monitor traffic and data that's flowing in and out. They gain visibility over all that is connected, on premises or in the cloud. As a result, agencies can track security threats and detect them sooner to cut off access and prevent information from leaking.

"The network is essentially the central nervous system of agencies' IT environments," Habtemariam said. "An intent-based network will help deliver an agile, multi-domain infrastructure that's going to allow them to enable a modern digital agency to drive innovation and efficiency."

3. Use the network as an on-ramp for cloud.

In the IT world, there's constant chatter about how cloud breaks down silos. But it doesn't do that, or provide accurate and actionable insights, without a cloud-ready agile network to support it.

A legacy network can limit visibility into data generated by remote workers and Internet of Things devices. Physical barriers would still define visibility boundaries, security would still depend on physical perimeters, and agencies' ability to leverage data "as a strategic asset" would still be limited.

That's why before ever going to the cloud, it's vital that agencies first assess the readiness of their network.

"In a nutshell, it's only through the network that the right data connects to the right users, to the right device, at the right time. And it ties back to the concept of enabling agility," Habtemariam said.

The Cloud During the Coronavirus Crisis

As the deadly COVID-19 made its way through the United States, the Centers for Disease Control and Prevention preached a steady slogan: **social distancing**.

Yet as businesses shut their doors and companies furloughed employees or told them to work from home, many agencies, lacking the technological ability to work remotely, asked that their workforces report to the office as usual. For at least 1,700 employees at the Health and Human Services Department's Office of Inspector General, however, telework in the name of social distancing immediately became the policy, all because of their office's prior investments in the cloud and its network.

"We had over 1,700 people with their laptops on concurrently yesterday, and with it, about the same number of mobile devices connected to the virtual private networks (VPNs) ... and from the overall inside of our network, it was really seamless," Chris Chilbert, the office's CIO, said in a late March interview.

Telework and remote work were top of mind when the office began its journey to the cloud and started expanding access to its network. So when the coronavirus hit and continuity of operations plans kicked in, calling for employees to telework and set up their own VPNs, it was no problem. HHS-OIG already had the bandwidth and cloud-based applications for the entire workforce to be online.

"Five years ago, we wouldn't have been able to pull this off," Chilbert said.

HHS-OIG is the largest IG office in the federal government, with its expansive workforce dedicated to fighting waste, fraud and abuse in health care. Due to the scope of HHS-administered programs, such as Medicare and Medicaid, the IG office has branch offices scattered throughout the country, some with just five or 10 people.

Five years ago, when going to the cloud, leaders targeted more remote work for employees in those smaller branch offices, which were expensive to maintain. The office also had sought out data backup and security to support telework in planning for crises.

"Contingency planning, we think, is very important," Chilbert said.

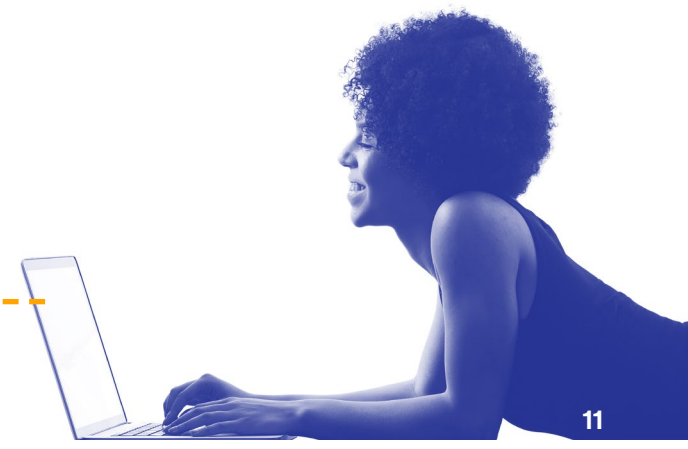
Before moving to the cloud, HHS-OIG felt the strain of regular network disruptions that a lagging on-premise system caused. The cloud allayed worries about what would happen if systems went down at the wrong time.

Other agencies didn't have systems in place to allow employees to work remotely when the coronavirus, which causes COVID-19, started spreading nationwide. Concerns about bandwidth or the inability to take work home tapered the Office of Management and Budget's staggered encouragement to telework.

Agencies were directed to continue operations toward the mission, and for many employees, that meant heading into the office – the only place they could get their work done – despite public health concerns. Many agencies submitted emergency budget requests to enhance their IT in hopes of teleworking.

But at HHS-OIG, the workforce had already been trained on how to use a suite of cloud-based tools carried over VPNs, so it was business as best as could be hoped for – all from home.

"These investments that we've made [have] really been powerful and enable us to work through this," Chilbert said.



INDUSTRY SPOTLIGHT

3 Keys to Scaling Fast, Avoiding Vendor Lock-In With Hybrid Cloud

An interview with Adam Clater, Senior Principal Architect, Red Hat's Public Sector.

Any movement to the cloud is a chance to get things right. Whether agencies are settled in or venturing out on their cloud quest, now is the perfect opportunity to reevaluate how IT operates and how it can be improved.

"Take the opportunity to get your house in order," Adam Clater, Senior Principal Architect for Red Hat's Public Sector, said. Red Hat is a leader in open source development, which many agencies are looking to as they try to collaborate and grow in the cloud. GovLoop recently spoke with Clater about three ways agencies can make cloud journeys successful.

By adopting standardization, automation and containerization, agencies are flexible and adaptable for the road ahead, whether they're crawling, walking or running to the cloud.

1. Standardize

Early on, agencies need to beware of vendor lock-in. Contracts that have vendors hold data without a clear entry or exit strategy can have drastic impacts in the long run, as cloud providers send a clear economic signal to consumers with pricing models. By evaluating the difference between network ingress – bringing data in – and egress – taking your data out – charges, you can identify where their priorities are.

It's always a good time to start standardizing systems on open standards and application programming interfaces (APIs). Using open source software, in which source code is made freely available, agencies can carry out infrastructure-as-code that exists universally, outside of vendors' purview. That way, developers don't have to start from scratch when agencies change cloud providers.

2. Automate

All systems can experience unscheduled down time, and quite often this is due to human error. Whether installing patches or conducting regular maintenance, one unintentional tweak can throw interconnected systems offline. But if all of this could be tested automatically, developers and operations teams could work toward bigger efficiencies without late-night blips.

Automation can run quality assurance checks before pushing software through to operations and automatically ensure version control in case of errors.

In the cloud, automation also saves a significant amount of time and, therefore, money. If a server has to be accessed to run maintenance or monitor an application, it's much more efficient to code these processes in advance so that they take a minimal amount of time to operate and can be turned off directly afterward. If your cloud strategy is simply a lift and shift of 24/7 workloads, Clater said, why not just get a managed services contract instead, which might be cheaper?

Thoughtfully automating workload deployment and life cycle is crucial to maximizing cloud investments.

3. Containerize

Containerization is a key enabler of hybrid cloud strategies and, while a good idea to automate and standardize no matter what, it's what truly taps into the potential of automation and standardization. Containerization is the packaging of all the resources needed for software development, operations and maintenance into one easily manageable digital bundle of code. Agencies can containerize and deploy their applications, then orchestrate those containers, with enterprise Kubernetes platforms such as Red Hat OpenShift Container Platform.

Because all of the resources are standardized in containers, agencies can run any of their developments across environments, while automation of these standard units makes agencies as agile as possible. Containers can include code that triggers certain chain events with other containers, and programs like Red Hat Ansible Automation Platform can help easily coordinate standardized protocols for automation.

Containers also allow agencies to scale workflows up or down easily, which is a major benefit of the cloud. The difference between sharing the code of containers five times and 100 is the push of a button. Clater said that means when it's tax season for the Internal Revenue Service, the agency could scale up, only to scale down later, limiting cost and duplicative work.

"Once an application is containerized, that means that you really met the 'nth' degree of standardization and automation," Clater said. "Because once something is containerized, we basically can stamp it out at any scale for any workflow."

5 Questions You're Afraid to Ask About Cloud

Whether or not you work in IT, cloud is changing your life. First, cloud popped up on the cutting edge of the private sector and trickled into your personal life, as we've seen society back away from DVDs and CDs in favor of popular streaming services such as Netflix and Spotify, made possible by cloud. Next, cloud started to transform common office environments, unshackling remote workers and catching government inboxes up to speed.

But as cloud is just starting to permeate so much of government, you might wonder why the delay. Is cloud unsafe? Is the workforce or are processes not ready? Does it cost too much?

We answer those questions and many more in the pages ahead, exploring how the cloud is changing office environments and the way government employees work.

QUESTION #1

Do I need to learn new skills or systems to succeed in a cloud environment?

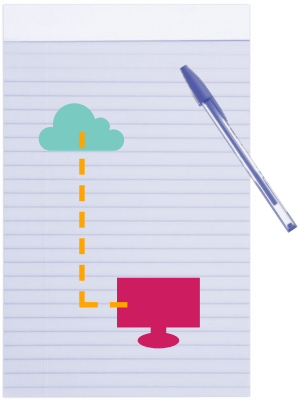
ANSWER: YES

What you do determines how much change there is ...

Cloud is always a change, and usually it's a pretty major undertaking for agencies. Although many employees may not see all of the work that goes on behind the scenes, the technology shift is a momentous step away from business as usual. IT, security and acquisition teams manage a metamorphosis from the technology of the last generation to technology from the next generation. Cloud bridges that divide, and all employees who are responsible for architecting cloud transitions require training, upskilling and time to get to know a new environment.

Meanwhile, employees in other functions who use the technology have varied experiences. The move can be quite jarring for them, as well, exposing the technological learning gap between last-generation applications and new processes and interfaces. Or, the move can also be pretty easy if their agency just lifts and shifts application, though even then, employees will have to know new logins, portals and processes. Either way, there's always some learning involved.

At successful agencies, leaders have taken their teams through the transitions by holding lunch and learns, on-site visits, forums and Q&A sessions to respond to employee questions and explain the why of transitions. There, leaders have addressed employees' concerns and noted their thoughts before the transitions began, preparing well-rounded cloud strategies to bring to the negotiating table with contractors.



THE NUMBER TO KNOW

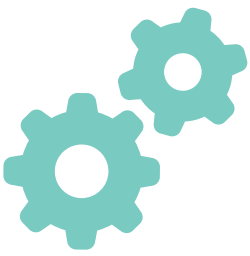
60%

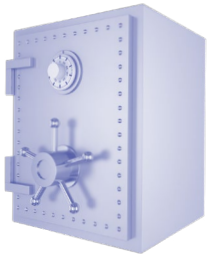
of government agencies use internal teams to lead cloud migration projects, as opposed to outsourcing to a vendor.

Source: Macquarie Government

THE CLOUD'S IMPACT

One process that cloud changes is software development. Cloud, because it's a shared system, opens the gateway to large-scale DevOps, a methodology whereby developers and operators collaborate throughout the lifecycle of software development, as opposed to working separately on different components. DevSecOps, which integrates security with automated testing, is also possible using the cloud and Agile practices.





AVAYA | Experiences That Matter

Connect, Communicate, Collaborate Without Boundaries

Transform your communications environment in the cloud with secure Unified Communications and Contact Center solutions that support true compatibility and limitless interoperability—with a clear focus on the reliability and security you need. Avaya FedRAMP cloud solutions provide you with the native benefits of the cloud along with the networking reliability and strength that Avaya inherently offers.

LEARN MORE

avaya.com

INDUSTRY SPOTLIGHT

The Key to Seamless, Uninterrupted Communication

An interview with Tim Shalvey, Director of Business Development, Avaya Public Sector

As the public sector has ramped up teleworking efforts because of the coronavirus, agencies have learned a few lessons along the way. And now, it's very clear that unified communications are fundamental in assisting the government in meeting its mission and citizens getting the services they require.

Whether interacting with constituents or coworkers, government employees need to be able to communicate seamlessly and securely in real time. That applies whether they're in a physical call center or at home.

"Agencies have long needed to enhance their telework capabilities. We believe this is going to change the way people work going forward," Tim Shalvey, Director of Business Development for Avaya's Public Sector, said in a recent interview with GovLoop. Avaya is a leading unified communication service provider for government.

Agencies' needs today will only grow going forward, with an estimated 21 million government contact center and unified communication seats as of 2019. The following steps will help agencies prepare for this future enterprise.

1. Use secure endpoints and certified solutions.

Some of the most valuable information that governments hold is transmitted through conversations, so phones and devices need to be fully vetted.

"With all of the cyberattacks that are prevalent in the world, we need to make sure in the government space that conversations are secure," Shalvey said.

Shalvey recommended that, where required, agencies go to hardened endpoints that meet federal security requirements. For example, agencies should rely on telephones authorized by their own trusted security officers. The National Telephone Security Working Group provides security officers with resources about unified communication systems that exchange sensitive government information.

2. Prepare to scale up or down.

The government has been going with on-premise systems for so many years now, many employees have become used to the feel of their devices. Although they want the newest technology, they don't want everything around them to change.

Agencies that work with Avaya can leverage existing unified communication assets as they move to the cloud. Agencies may utilize existing on-premise IT assets, for example, to maintain working analog solutions while connecting into secure cloud resources.

"They're familiar with operating their technology, so by using those existing devices and being able to bring them into the cloud, the end user experience doesn't change," Shalvey said.

Newer endpoints can also be delivered as a service where needed, which reduces capital and upfront cost. No matter where they are in their cloud journeys, agencies can avoid common culture and cost pitfalls when they transition existing assets to the cloud and fill in gaps using device-as-a-service.

3. Construct a resilient enterprise.

Once these endpoints are updated and placed in the cloud, agencies can build out a resilient, multichannel enterprise equipped for internal and external communications.

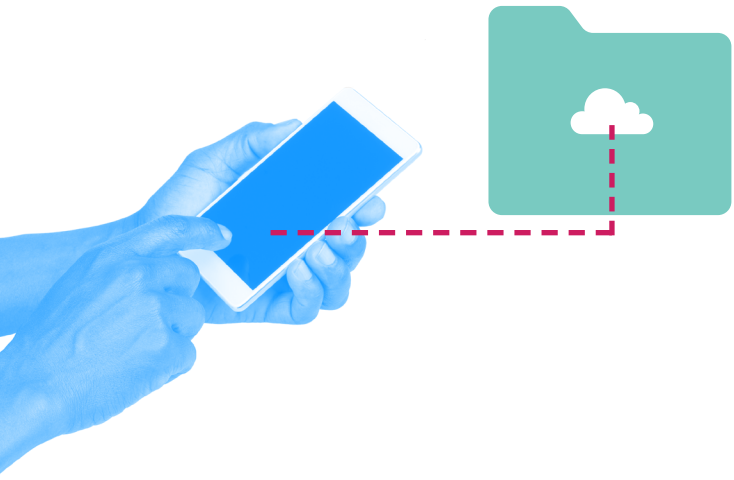
With these new channels, agencies are ready for virtual conferences that include audio, video and screen-sharing. Agencies can also deploy telehealth services.

By spinning up applications and providing back-up data centers, agencies are more resilient. In the case of physical harm to data centers, agencies can still securely maintain information-sharing and keep powering their mission forward because of uninterrupted communication.

"With modern unified communication channels, cloud-powered applications supporting telework speak to a very high level of resiliency for any agency," Shalvey said.

THE WORKFORCE IMPACT

Cloud's effect on employees outside IT, security and acquisitions is not nearly as profound, but going from a traditional, on-premise environment to new mobile and collaborative applications can still be weird for everyone.



To prepare the majority of the workforce, agencies can look to change management best practices. Employees need to know whom to call to ask about new technologies, but they also need to feel empowered exploring the options themselves.

The biggest change might not be in the technology itself but instead in related processes. If a folder can be hosted in the cloud and shared by multiple parties, maybe there's no longer the need for a weekly meeting to exchange information. Expectedly, when processes adjust to accompany the cloud, employees can see their jobs shift in favor of more telework and remote responsibilities.

These changes are often for the better. All they require to be successful is leadership offering resources – such as town halls and transition plans – to get people on board.

Bigger challenges can arise when workloads and outcomes aren't impacted. Change for change's sake sometimes happens when agencies feel the pressure to go to the cloud but don't know what they want to achieve, disrupting employees' regular workflows for no good reason.

THE IT AND SECURITY IMPACT

Cloud looks very different from the technology of old. Instead of wires and hard drives, everything is virtual, and that takes some getting used to for IT teams that have worked with physical technology their whole lives.

Similarly, security teams are no longer charged with focusing on the perimeter. As their jobs become increasingly data-oriented, they need to be fully prepared to use new dashboards, track connections and work alongside emerging technologies, such as AI.

When the cloud is introduced, roles change. Instead of physical maintenance or troubleshooting in an office backroom, those functions move online. And the only way to prepare for that is training.

IT teams can – and should – expect agencies to provide training on cloud, whether it's in-house or through the many certification programs that industry offers. Employees should enroll in necessary and appropriate training, which can range from cloud basics to deploying highly specific software, given agency backing.

Take the Transportation Department, for example. It actively sought out cloud training opportunities and created a webpage from which employees could access them. The department also looked to upskill or hire people with expertise in moving workloads to the cloud, offering pathways for employees to be ready for the new environment.

Elsewhere, employees who want a head start can get going on training preemptively, before agencies begin going to the cloud.

THE ACQUISITION IMPACT

For contracting professionals, buying cloud is unlike buying anything else. Instead of paying for 5,000 stamps or budgeting for $10,000 worth of conferences, cloud is a pay-as-you-go model. And that can lead to extremes.

If you've heard that cloud is significantly cheaper than on-premise solutions, it's true that it *can* be. For applications that are utilities or where transitions eliminate energy-inefficient storage costs, cloud makes a major difference. Cloud can also get rid of duplicative labor, support analytical capabilities and increase agency efficiency – all potential cost-savers.

But if an on-premise solution is a 24/7 application with high-volume usage, it's going to cost a lot to run in the cloud as is.

Furthermore, when purchasing cloud, ballpark price estimates are generally as good as it gets. Acquisition and IT teams need to communicate what services are the best use of agency resources.

The federal government currently has no standard model for buying cloud, but some state governments do and there are various resources available to agencies. But while agencies can join community groups and attend sessions, to really nail down what's best for cloud in their environments, IT and security teams need to be part of the acquisition process.

TIPS FOR THE TRANSITION

Bolster communication: Like it or not, cloud has a certain aura. When people hear it's coming into their office, all sorts of questions will pour in. As with any major transition, a best practice for addressing them is hosting community open-attendance meetings. In this free exchange of information, agencies can get the picture of peoples' concerns, misconceptions and ideas about the cloud.

Advocate for training: Cloud poses the biggest risk and opportunity to folks in IT. While other professionals will access and use the cloud, IT professionals will supervise and maintain an entirely new system that they can't quite put their finger on – literally. Before the transition, set aside and stagger out a few weeks for people with IT-related jobs to receive training on the cloud.

Accelerate your cloud journey

Government agencies are driven by the need for more speed and IT agility, which requires modernization, transformation, and re-platforming.

ServiceNow is committed to helping you identify which workloads work best in which environments, and determine the best fit of cloud services for your needs.

Remove the friction from your cloud journey and embrace the technology needed to accelerate your digital transformation.

Learn more at **www.servicenow.com/gov**

servicenow

INDUSTRY SPOTLIGHT

Facing Down the Biggest Challenge in Cloud Transitions

An interview with Jonathan Alboum, Principal Digital Strategist for Federal Government, ServiceNow

In the cloud, every new update is supposed to repair a glitch or fix a common problem. But what if the biggest challenge isn't technology, but something less tangible?

Culture is the first problem for every cloud move. When people resist training, cling to old processes or protest new policies, culture can single-handedly derail transitions.

"Either you do the transformation yourself, or you will be transformed," Jonathan Alboum, Principal Digital Strategist for Federal Government at ServiceNow, said in a recent interview with GovLoop. ServiceNow partners with government to deliver digital workflows that unlock productivity by creating seamless IT, employee and customer experiences.

Culture is the one constant throughout all governmental departments. While some might have better technology or more accessible processes, all face the same challenges in winning over people's hearts and minds. Alboum offered several practical and actionable steps for how agencies can solve the cultural dilemma.

1. Train and educate your leaders.

When agencies are considering the cloud, leaders must buy in to the overall direction. However, they may need help understanding what's involved.

"Leadership needs to understand the art of the possible when it comes to the cloud, because they're going to be the ones who ultimately lead the change," Alboum said.

A step that agencies should take is to educate senior managers, who need to understand what the cloud really is and how it will impact the average worker.

Next, agencies should learn from cloud providers that will engage with second-line managers to assess needs and readiness. With newfound knowledge, agencies can then begin targeted pilots.

2. Demonstrate the art of the possible.

Without careful planning, altering processes in preparation for cloud transitions might not be viewed as supportive by the workforce. It could actually leave the opposite impression.

Forcing employees to change rarely works. Instead, employees need to see what their new reality will look like, buy into the change and assume control themselves.

"It starts with sharing a vision with your employees, showing them how it works, and giving them a chance to feel and touch it," Alboum said.

The best way to do this is for agencies to embrace platform technologies to quickly deploy cloud solutions for high-value workflows, such as employee and contractor onboarding and offboarding, he said.

"Once the organization experiences the speed and ease of creating cloud-based digital workflows, magic happens," Alboum said.

As employees interact with the new systems, they're empowered to suggest policies and processes for the cloud. This in turn drives leaders to really understand how their data and work move through the agency.

Suddenly, employees are engaged in decision-making, and as they innovate, agencies don't have to fear cultural tumult. The organization instead becomes more resilient as it undergoes a digital transformation.

3. Make the adjustment easy.

Of course, it's not that simple. Agencies must consider cost and complexity when choosing cloud solutions, and the resulting inconsistency of multicloud environments can derail the envisioned end state. Usually, that's unavoidable.

But agencies can still integrate the cloud experience as much as possible with several techniques. "Going to platforms, instead of stovepipe applications, will improve user experience," Alboum said. He also recommended finding a solution, like ones that ServiceNow provides, to orchestrate security and functionality across these different cloud platforms.

With orchestration, employees can use one login and maintain the same primary interface, even across multiple clouds.

"Those things are force multipliers for these kinds of transitions," Alboum said.

An easier transition means better efficiency. By helping the workforce adjust, agencies are really helping themselves capitalize on cloud.

QUESTION #2

Does cloud really offer all the capabilities that advertisements promise?

ANSWER: YES

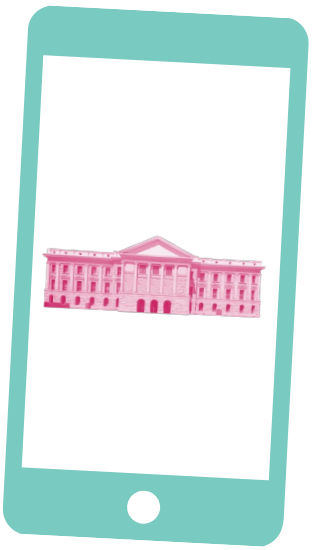
Your agency might not be ready for all of them, though ...

You've probably heard the phrase "cloud is an enabler," and yes, it's true.

Without the cloud, apps would not be as personalized and data wouldn't be as accessible. Without the cloud, live stats and instant collaboration wouldn't be possible. And without the cloud, Airbnb and Uber wouldn't exist. Cloud truly enables all of these amenities of 21st-century life that we've become accustomed to.

So, does that mean that we'll soon see similar apps and capabilities in government? Yes and no, on a case-by-case basis. Government trails the private sector in several areas – some for good reason, related to privacy or security – that naturally stifle its ability to make the same advances. For example, in the federal government, websites need a standardized appearance in order to ensure authenticity, accessibility and reliability for citizens. Agencies can't be as experimental in designing interfaces.

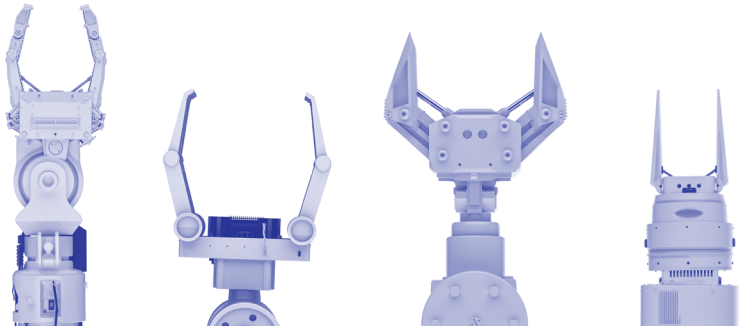
However, we have already seen governments begin to take advantage of easy-access cloud capabilities. State governments have paired up with voice response systems to launch apps, and many federal inboxes use Microsoft Office 365, a standard in the private sector as well. Governments now, because of how operating models change with the cloud, have the opportunity to escape legacy frustrations and unlock more of these same capabilities – even if to a slightly tempered degree.



WHAT CLOUD HELPS WITH

Automation: Agencies can acquire automation capabilities in the cloud. Automation is when a coded software completes manual work that people traditionally do. An example of automation is developing programmed security responses to hacks, so that software would carry out the action as opposed to a person. Although the cloud is not necessary to deliver automation, it can be a useful vehicle as data flows instantaneously through the cloud and between applications for faster action.

Collaboration: Agencies can gain access to central collaboration tools, such as shared calendars, agendas and notes. Whereas these capabilities may have been impossible to host when relying on on-premise storage, the cloud gives access to all authorized users. These sorts of technologies can increase productivity and help develop a single source of truth.



Emerging Technology: Agencies can unlock a suite of emerging technologies, such as AI, when going to the cloud. Beforehand, these capabilities might have been out of reach because of upfront investment, technical debt or a lack of usable data. With the cloud, however, agencies can buy highly advanced software-as-a-service suited to their needs. By combining data storage and modern capabilities developed by industry for the many, cloud can open new doors for agencies. If these programs constantly run on large databases, however, they can get costly.

Data Tools: Agencies can count on a more shared and centralized base of data in the cloud. The cloud can automatically sync the information it holds, so many times, employees don't have to retrieve or standardize data. Cloud-based data solutions are secure – with monitoring and access controls – and they can include a variety of tools so that agencies can control where data goes, who owns it and how it can be used. From these sources, technically known as data warehouses and data governance solutions, agencies can start to develop models of predictive analytics or neural networks, which recognize and connect patterns in data. The availability of data is a differentiator of the cloud. In comparison, siloed data center storage would separate data based on physical location or servers.

TIPS FOR REACHING CLOUD CAPABILITIES

Diagnose what you need and what you want: All of these capabilities sound amazing, but remember, they're not free. Before investing too heavily, it's best to have a multistep plan for cloud maturity in mind. Cloud can either be an accessory or a foundation for agencies, and both options can work, given the right circumstances. But agencies that invest in the technology without a clear plan are likely to fail to capture major benefits and waste money and time on a poorly executed transition.

Run a pilot: Before buying the bar, start with just one workflow or dataset. By tinkering with the capabilities in the cloud, you can get a better sense of what suits your agency and workforce. You'll also be able to see what connections are easy to make to existing systems and which might be more difficult.

Don't jump in headfirst: If agencies go gung-ho to the cloud, they're likely to abandon working, effective, on-premise solutions in favor of cloud-based tools that might be more ill-fitting. Not everything is made for the cloud. Dip your toes in and see what best suits your needs.

WORD OF WISDOM

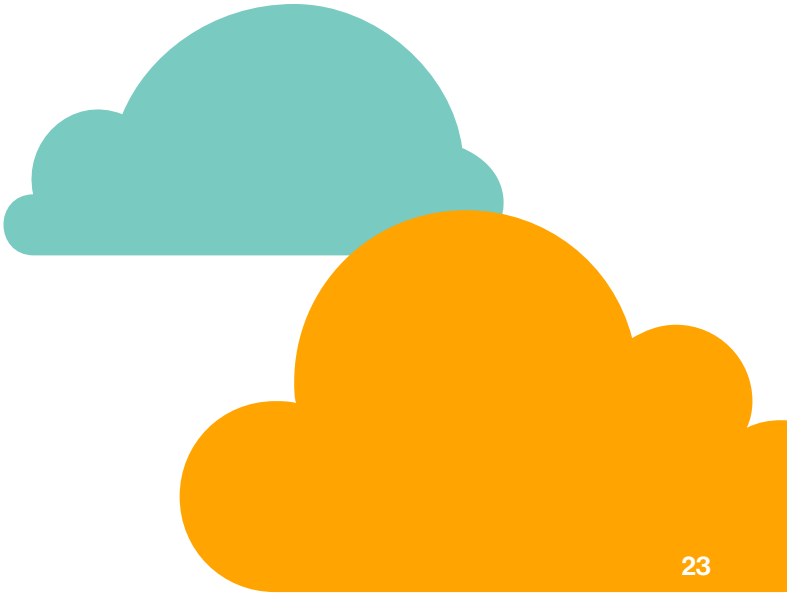
Remember, these are capabilities, not guarantees. Many agencies may see only one or two of these benefits in the cloud, while some will see more and some will see less. The point is that the technology is there, but whether agencies have the ability, budgets and processes to reach these capabilities is a real question.

THE NUMBER TO KNOW

15 of 16

agencies surveyed by the Government Accountability Office (GAO) in 2019 "identified significant benefits from acquiring cloud services, including improved customer service and the acquisition of more cost-effective options for managing IT services."

Source: GAO



INDUSTRY SPOTLIGHT

Beyond Storage – Data Freedom in Complex IT Environments

An interview with Nick Psaki, Principal Engineer, Pure Storage Federal

Data wasn't meant to sit dormant in the cloud. Nor was it meant to be saddled up with one storage provider and shooed off to the horizon.

As agencies' IT environments are in a constant flux, data should be the foundation of consistency, because without accessible and available data, organizations can't hope to attain the best of up-and-coming technologies — no matter how flashy and geared-up they are.

"If you build a high-performance car and put bicycle tires on it, you're going to get bike-level performance no matter how hard you try," said Nick Psaki, Principal Engineer for the Federal Division at Pure Storage, which provides data service platforms for on-premise and cloud environments.

GovLoop recently interviewed Psaki about the importance of data availability in hybrid cloud environments. He said that for modern IT to succeed, data needs to be at the core of agencies, both on premises and in the cloud.

The three points to follow will help agencies keep the wheels rolling on modernization and mission endeavors.

1. Platforms should be simple.

Sticking with the car analogy, in a NASCAR race, pit crews routinely have to change out tires and provide maintenance. But while the focus of the sport is driving, bad pit stops are equally as damaging as poor performance on the road.

When agencies are getting data service platforms in place, they need to be sure that they're not stuck in neutral, trying to figure out platforms while they have work to do. The pit stop should be quick, so they can get back on the move. In tech terms, that means every maintenance or upgrade project must be non-disruptive to operations, and systems should require very little effort to install, operate and maintain.

Any system should be simple – built for users whether the data is on premises or in the cloud. Simple means more intuitive, quick and easy to use. Otherwise, the next time agencies reconsider their IT infrastructure, they'll interrupt business by reconfiguring the system all over again.

2. Platforms should be seamless.

With all of the hype around cloud, on-premise infrastructure is often viewed as the government IT stepchild. It shouldn't be.

On-premise applications and storage remain the preference for many different situations.

Any data service or storage platform that's built for the cloud should also work on premises, with the same functionality and integration. Very few organizations truly have everything in the cloud, so when organizations ignore on-premise systems, they also ignore important data and functionality.

Most organizations remain in a hybrid cloud state, and they will for the foreseeable future. Data service platforms should be flexible enough to gel in any environment, not corner agencies into an IT layout that doesn't work for them.

"It also allows you to avoid a vendor lock-in trap, by having some say in how your data gets managed and migrated," Psaki said.

3. Platforms should be sustainable.

Times change, and just because content grows older, it doesn't mean that it becomes less valuable. Think about your favorite home videos or movies. The same movie can be stored on VHS tape or DVD, and the only difference is the technology has been updated.

Data storage and service are similar. Agencies need to seek out platforms that grow with the times and bring the data with them. Pure Storage, for example, delivers its data service platform through software, and it will automatically update the system hardware as a part of the maintenance subscription to match the newest model. The result is a system that is perpetually sustained and improved over time, at no additional cost.

When everyone is working from the latest and greatest version, using a vast base of data, agencies can explore historical trends and dive deeper into analysis.

"Data is long-lived. And making data available to use cases that we didn't even envision five years ago or 10 years ago has become a significant challenge for organizations," Psaki said.

Question & Answer With SBA's Guy Cavallo

SBA is looked to as a trailblazer for cloud in government. Under the leadership of Deputy CIO Guy Cavallo and CIO Maria Roat, SBA maneuvered its enterprise to cloud while responding to small businesses' needs following Hurricane Maria in 2017. Since then, SBA has prioritized going to the cloud as much as possible, and the small federal agency has gained business insights and accumulated cost savings because of it.

The following Q&A is from a March email interview with Cavallo. His answers have been lightly edited for clarity and length.

GOVLOOP: What questions did employees have when cloud was first discussed? Was there any apprehension?

CAVALLO: The first questions were: Which cloud? Would we move everything? How fast would we do this? Yes, there was apprehension because it was a change to the status quo. We overcame the apprehension by hosting weekly lunch and learns, sending staff to cloud hands-on training sessions and providing additional training.

What sorts of jobs underwent the most change, if any stand out?

Any job that was focused on purchasing data center hardware was the most affected. Those that enjoyed purchasing CPUs, storage, etc., had to learn to give that up. The next most affected were the Security Operations Center staff as we leveraged the cloud and implemented AI to help them see increased visibility into the organization.

Do employees have to learn new skill sets, like data analytics or machine learning, with the cloud? Or even if they don't have to, should they?

It depends upon their work. We do need new skill sets, such as understanding virtual machines and costing models in the cloud – ideally, someone who can do both. We also needed improved skill sets in establishing virtual networks, security boundaries, and evaluating what can be turned off and on and when – things that were not skills needed with a traditional on-premise data center.

What are the challenges of cloud technologies that many don't consider up front?

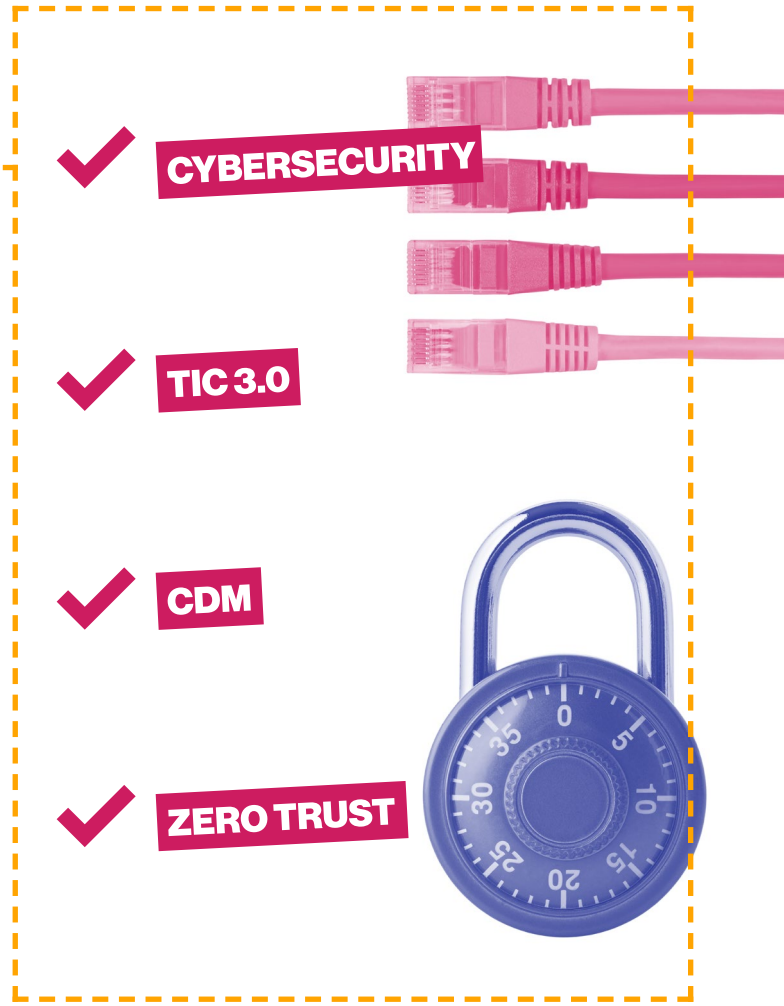
I have had the luck of leading the implementation of the cloud at two agencies, the Transportation Security Administration and SBA. The biggest challenge in both of those efforts was the difficulty and length of time it took to establish new large network connectivity to the cloud. It took longer to do that than it took to launch the cloud efforts. In talking about this with other federal agencies, I heard this same challenge from everyone else. It wasn't just my experience.

What is new with SBA's cloud journey in 2020?

Our next step is to continue to evolve our cybersecurity capabilities by gaining approval and implementing a cloud-based TIC 3.0 solution, and continuing to work with the Homeland Security Department on how the cloud can improve the Continuous Diagnostics and Mitigation (CDM) program. We are in the early stages of implementing a zero trust network, which will make it easier for us to secure and keep the SBA network up and available.

What best practices or advice do you have for employees who are adapting to cloud, either in its adoption or continuing along its journey?

Be prepared for change on a daily basis. Use Agile to implement the cloud because if you do it waterfall, the cloud will change by adding new features or other changes before you finish. You don't need an army to get started. At both agencies, I launched the cloud in less than 90 days with just a handful of staff.



Search. Observe. Protect

Elasticsearch Service is FedRAMP "In Process" on AWS GovCloud

For all your mission-critical use cases

- App Search
- Observability
- Security

Start your free trial at **elastic.co/campaigns/govcloud**

INDUSTRY SPOTLIGHT

The Capabilities That You Should Ask for in the Cloud

An interview with Anurag Gupta, Principal Product Manager, Elastic

Recently, government IT has met its gravest challenge in years, as the novel coronavirus has disrupted business as usual and put tremendous strain on systems and networks. Although agencies have worked to do the best they can, some IT systems just can't meet the moment.

But cloud solutions can give government workers and their agencies the scale and flexibility to rise to the challenge.

"Cloud gives you a benefit in terms of scale and acceleration, allowing agencies to focus on their mission instead of installing and operating software," said Anurag Gupta, Principal Product Manager at Elastic, in an interview with GovLoop.

Elastic offers secure cloud solutions with three critical functions for the public sector: enterprise search, observability and security. Gupta shared his advice for how to use these capabilities.

1. Enterprise Search

With cloud-based systems, searching is no longer a siloed activity kept to individual hard drives and servers. IT personnel can instead search through entire systems for what they need, when they need it.

In times of high demand, such as when citizens are submitting more forms, agencies can scale up to meet requests in the cloud. Then, with enterprise search capabilities, they can quickly prioritize and respond.

For example, the city of Portland, Oregon, website is used to host public content, support online payments and more. By implementing Elastic Enterprise Search, the city was able to get started in hours enhancing search performance and providing a better citizen experience.

2. Observability

If on-premise servers are near capacity or an influx of users is slowing down applications, agencies should know without having to check manually.

An observability solution tracks system health, memory and behavior in one place – for on-premise environments and cloud deployments alike. With a cloud observability solution, agencies can monitor applications and feed metrics back to application and IT teams with a highly available and scalable solution, growing as agency data does.

"Elastic Observability allows users to navigate logs, metrics and application performance management seamlessly from a single interface. Cloud simplifies how agencies can deploy and how they can scale for growing datasets," Gupta said.

3. Security

IT and security teams shouldn't have to spend months setting up a new system and synchronizing it with applications and devices. Right out of the box, agencies should expect encryption, monitoring, authentication and detection tools.

Security is not only about configuring best practices, but it's also about empowering agency employees with tooling used by threat hunters and security practitioners. Cloud can democratize that availability and make it easy to deploy within an organization.

"Elastic ensures that all the security best practices are taken care of and also includes a SIEM for all deployments. With Elasticsearch Service on Elastic Cloud, you get encryption at rest, security enabled for all of your clusters and SIEM enabled. And our AWS GovCloud offering for government users is FedRAMP 'in process,'" Gupta said.

Combining enterprise search, security and observability solutions in the cloud propels government IT departments to modernization. The cloud delivers speed, simplicity and scale, especially when agencies need these capabilities the most.

QUESTION #3

Is cloud always worth it?

ANSWER: NO

There's a lot to consider ...

When agencies calculate the worth of a new program, they have to account for all kinds of factors. Cost is the most obvious one, but they have to consider workforce, security, processes and service delivery as well.

With all of this in mind, cloud comes with its pros and cons. While an as-a-service model sounds like a cost-saver across many lines of business, agencies shouldn't just pick and choose the most affordable option every time. If they did, they'd wind up with a menagerie of technologies – some on premises, some in the cloud and all with next to no ability to communicate with one another. Many cloud experts will warn you of multicloud sprawl, which leads to inconsistent policies and data practices.

That's not to say cloud won't be the best option many times. During a crisis, if a county needs to spin up an interactive portal for tracking and securely sharing health data intergovernmentally, cloud is the most efficient way to do so since governments can run off a shared system. Cloud could also save money because the system will not always be on.

The same level of data aggregation in real time could not be kept up with an on-premise solution, which would have taken longer to generate in the first place anyway.

However, high-volume, high-usage programs that work effectively might be best kept on premises, especially when employees are familiar with the system.

Costs can also add up if agencies indiscriminately put all of their data and applications in the cloud without considering hidden costs, such as entry and exit fees and the expense of network upgrades. These hidden costs can plague agencies and doom cloud transitions. What's more, if employees lack proper training when cloud is implemented, productivity can fall off, too.

COST AS A UTILITY SERVICE

"Just like electricity or your water bill, if you turn it on and keep using it, you can surprise yourself with a big bill. So make sure that you have appropriate controls in place to manage your usage of this resource."

– Chris Chilbert, CIO, HHS-OIG

THE NUMBER TO KNOW

84%

of cloud investments that GAO reviewed did not show savings. GAO said this is the result of agencies' difficulty in tracking information, not tracking information because it wasn't required or because the cloud had not directly resulted in savings.

Source: GAO

WHAT'S GOOD IN THE CLOUD

The good news is that with the right processes and preparation, much of agencies' technology can thrive in the cloud. Email is one of the most common migrations in government, and that alone has increased productivity and collaboration. But more than email, a lot of applications, data and systems are better off in the cloud.

SBA has made cloud its default, and the agency has seen tremendous returns in cybersecurity, AI and efficiency because of it. Having the cloud across its network and applications provides SBA with enterprise cybersecurity visibility, letting the agency detect more attacks and plug holes in its network. And with that increased visibility, SBA uses AI to protect assets.

Moreover, data tools fit ideally in cloud environments for several reasons. For one, the cloud stores information in one place, so analysis is conducted on larger, more valuable datasets. The cloud also gives neural networks and AI easy access to data, meaning that the technologies can be put into place without lots of coding or software development.

HHS-OIG has seen all sorts of new data capabilities in the cloud, including AI and better control of its data. The office also has gained more understanding of its information because employees can collaborate for data-based projects, including predictive analytics.

Finally, the cloud is also important for backing up systems and sensitive information. If ransomware or a cyberattack compromises a data center, the information could be lost for good. In the cloud, however, agencies can have copies of all of their information available so that if an attack does land, at least the data won't be obscured or lost.

WHAT'S GOOD OUTSIDE THE CLOUD

Still, other agency assets are best kept in old, reliable data centers. For example, HHS-OIG maintains an on-premise solution that monitors its infrastructure's health without ever turning off. Because it ingests a large amount of data and is never offline, this solution is more cost-effective to have on premises. Similar applications might also make more sense to keep out of the cloud.

Additionally, some agencies are just working with limited budgets and lack the resources to move major portions of their existing IT to the cloud. In these cases, they should keep trusted and well-functioning on-premise solutions in place, and only look to the cloud to troubleshoot particularly problematic workflows or experiment with new capabilities.

Both Cavallo and Chilbert said that upgrading their networks came before the cloud, and that took most of the investment up front. They also both started with relatively small deployments in the cloud before looking to revolutionize their IT environments. Until proving how cloud fits into the existing IT picture and preparing networks and processes, agencies are better off going for small, non-mission-critical elements. Going too big too fast is one of the biggest pitfalls for cloud transitions.

TIPS FOR MAXIMIZING CLOUD

Start small: A maxim for IT projects, "start small" applies to cloud as well. Think of an instance where it could be useful and try a proof of concept. Starting with a tightly knit team on a low-risk project helps reimagine workflows and processes, see how cloud works and estimate costs for when it's time for a bigger endeavor. Beginning this way can also coordinate IT, security and acquisition best practices.

Make sure your network is ready: The cloud will bring new devices and network connections into the picture. TIC 3.0, the federal network cybersecurity guidance, offered a cloud use case for just this reason. Before putting applications and systems in the cloud, beef up your network to open up access. Otherwise, the transition can quickly lead to lags and lack of bandwidth for mission-critical elements.

INDUSTRY SPOTLIGHT

Simple Steps to Security in the Cloud

An interview with Nicci Neal, Principal Business Development Manager, Amazon Web Services

When shopping for furniture online, people usually look at several factors – price, reviews and dimensions, just to name a few. But another consideration is the ease with which the furniture can be built.

The same is true with the cloud. In recent years, agencies have become more cognizant of the cloud and its potential benefits, but the comfort of the status quo still beckons.

After all, moves to the cloud require agencies to prove that they are meeting compliance requirements all over again, in addition to satisfying their own security departments. Or, so it would seem.

"They may be looking at solutions that can very quickly get them through FedRAMP," said Nicci Neal, Principal Business Development Manager at Amazon Web Services (AWS).

The AWS GovCloud (US) Regions are compliant with several major U.S. government regulations including FedRAMP, which vets and assigns security levels to vendors' cloud offerings.

Neal spoke with GovLoop about how to expedite moves to the cloud while maintaining security and compliance. She offered these best practices.

1. Don't oversell on-premise security.

People often talk about how they felt more secure having applications in their data center, but on-premise systems had their own security challenges.

For example, shadow IT, unapproved systems or services introduced by employees that circumvented security policies, came on premises. Shadow IT is rarely introduced with malicious intent. Because it's hidden from security experts, however, it leaves applications and data vulnerable. While cloud doesn't eliminate shadow IT, it allows agencies to take greater stock of what's in their IT environments so that they can secure them.

Cloud providers like AWS can help provide centralized visibility and management of customers' environments with resource tagging to track access. Moreover, with software solutions found on AWS Marketplace, agencies can standardize their baseline security configurations and manage configuration drift.

"Security does lead every decision that we make, from the design and build phases all the way through operations," Neal said. "And that's where our customers want to go."

2. Seek out ways to accelerate compliance.

Compliance does not have to be the chore it was on premises. Agencies can design in cloud regions like AWS GovCloud (US) to meet governmentwide compliance and security standards faster by moving out of data centers and inheriting readymade security controls. They also gain greater control of their networks and overall security posture, even just by preparing for hybrid cloud.

Relying on cloud compliance programs like FedRAMP, agencies can see where secure and approved offerings fit into their own architectures. The AWS GovCloud (US) Regions, for example, are authorized at the FedRAMP-High baseline and align with NIST, ITAR, DoD SRG, DFARS, CJIS and other federal compliance models. Looking forward, AWS GovCloud (US) will also meet DoD's Cybersecurity Maturity Model Certification (CMMC), which examines vendor supply chains' security.

To speed up compliance and acquisition processes, agencies can also look to shared responsibility models. With terms defined in advance, agencies know what they have to manage security for, such as data and access – and what they don't.

3. Ready the workforce and IT operations models for cloud.

Lastly, agencies need to make sure that they're ready for cloud. Adhering to sound security policy is good for the higher-ups, but workforces still need to be trained on the tools and applications needed for the new environment.

AWS offers widely enrolled-in training courses, which cover standards, compliance and security. Agencies' workforces can receive customized training as well.

When workforces know how to operate in the cloud, not only is the environment more secure and compliant, but it is also more productive. Agencies can bring readymade automation into secure development and operations models, such as DevSecOps, to speed up application rollouts and meet compliance requirements.

"Those benefits are really great for customers that are looking for pre-scripted guidance and meeting compliance," Neal said.

QUESTION #4

Is cloud safe for my data and me in the face of cyberthreats?

ANSWER: YES

You still own the information and its security ...

Ask anyone in government IT, and one of the most common questions about cloud that you'll come across is if it's safe. When SBA and HHS-OIG met with employees before their moves to the cloud, the most common question they received was how the cloud would be secured – asked in a variety of ways.

Human nature suggests that people feel safer when they're in control of their outcomes, even if plenty of examples to the contrary rebut the idea. People remain far more afraid of flying than driving, despite traffic accidents' far higher fatality rate. And employees seem far more concerned about cloud security than the status quo, despite frequent breaches of government on-premise data, including government's most infamous breach.

The 2015 cyberattacks on the Office of Personnel Management exposed the information of more than 22 million people after infiltrating an on-premise system. The breaches remained undetected for months, and some in the business of data protection have said that cloud-based monitoring and defenses could have alerted the agency sooner to staunch the data hemorrhage.

That's not to say there shouldn't be questions about cloud security, as many concerns stem from uncertainty about the protection of servers employees can't see. Who's responsible for data in the cloud? What happens to data when agencies want to move to a different contractor? Is the physical security of data guaranteed?

Different government provisions answer these questions, such as the Federal Risk and Authorization Management Program (FedRAMP) at the federal level, while state and local governments often have their own. Meanwhile, government-approved clouds often already include best-in-class security measures, such as multifactor authentication and holistic monitoring, from the vendors' side. While not a panacea for bad security practices within agencies' realms, cloud is no less secure than data centers. In many cases, it's more so.

With that being said, cloud ushers in plenty of new processes and a new operating mindset, which can present more modern challenges. These new processes emphasize the establishment of trust zones and shifting the focus from security on the perimeter to locking down access to important data wherever it is. Cloud is a reason for and component of these modern security tenets, so agencies do have to adapt.

A NOTE OF WARNING

Capabilities and regulations are part of a cloud security blanket, but those alone can't prevent attackers from initially accessing systems. Agencies still need to emphasize security within their enterprise, requiring strong best practices and training employees. Handing off information to cloud service providers doesn't mean the information is safe or in danger; it's up to agencies to put the right policies in place and it's up to employees to exercise correct judgment.

THE NUMBER TO KNOW

17%

of states are using specific cloud procurement and contract templates.

Source: NASCIO

GOVERNMENTWIDE MEASURES

Governments all have their own ways to ensure cloud security. In the federal government, FedRAMP authorizes and rates government clouds so agencies can quickly procure safe solutions. By authorizing clouds as safe for high, medium or low impact, FedRAMP gives agencies a good idea of what security measures they need based on the type of data they're guarding. "High impact" means that the cloud is secure enough for DoD systems. State and local governments can also use FedRAMP as a guideline for the security of approved solutions.

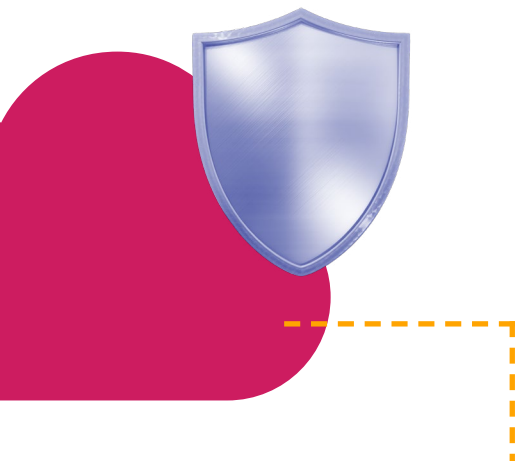
While questions of vendor risk are very much relevant in the acquisition process, fortunately, approval requirements usually ensure that vendors are in resolute financial standing and trustworthy to live up to contract requirements. What is left to be ironed out are terms of risk ownership, data deletion and built-in security measures. Many agencies are working to address this up front.

Delaware, for example, has the following terms and conditions for cloud service providers:

- A negotiated plan for contract termination, assistance in restoring services and data, and data disposal
- A requirement that any breaches must be reported to the state within 24 hours of discovery
- The state's full ownership of data
- Data modeling and password protections

Chilbert said that training staff in how cloud security is different from on-premise security is a must. Agencies can go about that by following National Institute of Standards and Technology instruction and complying with the Federal Information Security Management Act.

The latest TIC guidance also supports cloud models, and CDM – designed to step-by-step improve the visibility of data, users and action on federal networks – is adapting to do so with SBA's help. These are signs of the times, as governmentwide, programs constantly tilt to accompany more cloud focuses, including the emphasis of data protection as opposed to perimeter protection.



TIPS FOR KEEPING CLOUD SAFE

Train all employees: Security is different in the cloud, and cybersecurity professionals should be certified and prepared for incoming policies and responses. However, with more endpoints available to hackers, employees also need to understand the role they play in cybersecurity. By creating strong passwords, recognizing abnormalities and upholding cyber hygiene, every employee can make a difference.

Avoid cloud sprawl: Preventing unnecessary cloud sprawl will also limit inconsistent policies and allow for holistic monitoring. Naturally, there will be differences in how cloud service providers secure data, no matter how consistent negotiations are. The fewer solutions, the easier it is to monitor data and standardize policies.

Negotiate clear policies: Financial responsibility, ownership and mandated security policies should be explicitly defined in contracts. Additionally, agencies need to think ahead, including measures for exit and entry plans to protect their data and financial interests.

POSSIBILITIES FOR CLOUD-BASED SECURITY

Cloud-based security opens the door to modern solutions. SBA has incorporated AI to protect assets and monitored its entire network with cloud, producing constant reports on who is accessing systems from where. That holistic approach to security can help the agency catch and negate threats quicker.

As the federal Cloud Smart strategy notes, cloud also supports identity, credential and access management (ICAM), which is policies that secure users' profiles and permit them access only to the data they're authorized for. Encryption, meanwhile, can lock down important files and data so that only those with the right key can see the information. Between AI-delivered security responses, ICAM and holistic monitoring, the cloud offers agencies the chance to move into a modern security state while promoting productivity across the enterprise.

SECURE PRIVILEGE. STOP ATTACKS.

ACROSS THE ENTERPRISE · IN THE CLOUD · ON ENDPOINTS

Unsecured privileged accounts add risk to your business anywhere they exist - 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise - on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networthiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- FIPS 140-2
- NIAP certified

Learn about our Federal capabilities at:

CyberArk.com

CYBERARK®

INDUSTRY SPOTLIGHT

Mastering the Role of Gatekeeper in the Cloud

An interview with Kevin Jermyn, Manager of Federal Engineering, CyberArk

When agencies go to the cloud, they usually do so with aspirations of more efficiency and new possibilities.

Security's job then is straightforward: Keep everything safe, and stay out of the way.

The problem is, that job isn't so easy to execute when you factor business realities into the equation. For as many cloud vendors as there are that boast powerful and effective security solutions, agencies still go to multiple clouds because of cost and technical debt, creating an inconsistent landscape of security.

This danger is especially pronounced when it comes to tracking users. As users bounce in and out of different workflows and multiple clouds, agencies need a way to enforce that these accounts are only accessing what they're authorized to. This is known as privileged access management.

"We're looking to ensure that people have the tools to do their job, and nothing more," said Kevin Jermyn, Manager of Federal Engineering at CyberArk. CyberArk specializes in privileged access management and can work with multiple cloud providers simultaneously.

In an interview with GovLoop, Jermyn provided three ideas for how agencies can make sure that access is secure in the cloud.

1. Install multifactor authentication.

For starters, there's no need to increase systems' exposure. Portals that are meant for internal use should be left locked down on the web, as public access to those systems increases the chances that a hacker will get lucky.

Agencies also have to continue promoting security on the edge, even as mobile security becomes more complex. Installing multifactor authentication, whereby users not only need a password but another form of identification such as a texted code, is a must.

2. Remember nonperson entities.

One of the largest benefits of cloud technologies is that users can introduce automation to the broad portfolio of data that they now have. Robotic process automation (RPA), specifically, is a coded computer software that performs repetitive, mundane activities that do not require high-level thought.

For RPA to work, however, it needs to access different systems, which often are hosted by different cloud providers. If processes are interrupted, RPA's value is limited.

"When we talk about credential sprawl, it's both a security problem, where it presents a lot of risk for a breach, but also an operations problem, where you're now managing credentials and identities across all of these different systems," Jermyn said. "That's a lot of administrative overhead."

By flexibly credentialing RPA bots to access all the systems needed in their workflows, agencies can prevent any snags in their delivery. Then, agencies and workforces can truly reach their full potential.

3. Incorporate automation into privileged access management.

Just like automation can be used to accelerate business operations, it can also be programmed into security responses.

A major threat to government security is when agencies fail to decommission credentials of contractors, part-time workers or employees who no longer require access to a project. Privileged access management can step in during these situations.

Additionally, successful access solutions can trigger stopgap measures to withhold access if a breach is suspected. If a user's profile has abnormal behavior, agencies can cut off access to files so that no information is compromised.

"If you're doing all the identity access management and privileged access management pieces manually, you're losing a lot of the benefits that come with digital transformation and moving to the cloud," Jermyn said.

QUESTION #5

Will the cloud transform how I use technology in government?

ANSWER: MAYBE

The technology is ready, but is government?

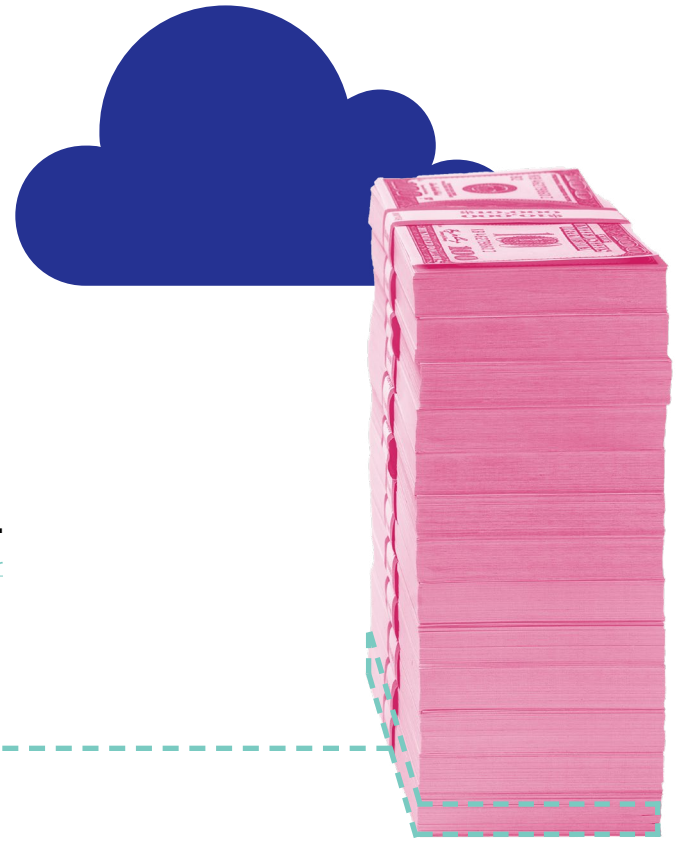
Far from genie-as-a-service, government clouds have been bottled up by legacy systems, and agencies are still grappling with whether to buy the cloud, what to use it on and how to maximize it.

Cloud is not the current state of government IT, although there are exceptions. SBA has realized tremendous cost savings, increased efficiency and redefined its cybersecurity approach because of its cloud emphasis. Meanwhile, HHS-OIG has enabled a workforce capable of being entirely remote by going to the cloud and putting in the legwork.

How did leaders in the field get to where they are, and why can't every agency just follow those same steps? Cloud adoption isn't uniform in government, and bigger agencies can struggle to go to the cloud as easily. The foundations of cloud – smarter processes, network expansion, creative acquisition, employee training and modern security – are more difficult to implement agencywide across large-scale organizations. As the Veterans Affairs Department and DoD roll out enterprise clouds to meet their workforces' needs, lessons learned can illuminate the path to cloud for other agencies.

Ultimately, the success of cloud won't depend on the technology. The technology is there, mature enough for all agencies to benefit from it. Instead, the foundations agencies have in place will determine whether employees will experience cloud as the go-to IT at their agencies.

NUMBERS TO KNOW



22%

of national governments' IT spending is spent on cloud. 20.6% of state and local governments' IT spending is spent on cloud.

Source: Gartner

2%

of U.S. agency-reported IT spending was spent on cloud in fiscal year 2018.

Source: GAO

RECAP:

THE FOUNDATIONS OF CLOUD

Smarter processes:
For cloud to truly be transformative, processes need to match cloud workflows. By removing silos and prepping data for collaboration, agencies can embrace the cloud.

Network expansion:
One of the first things agencies must do to welcome the cloud is expand their network connectivity, creating more space on the spectrum for new devices to join. Although a lot goes into this process, without a wider network, the cloud isn't worth it.

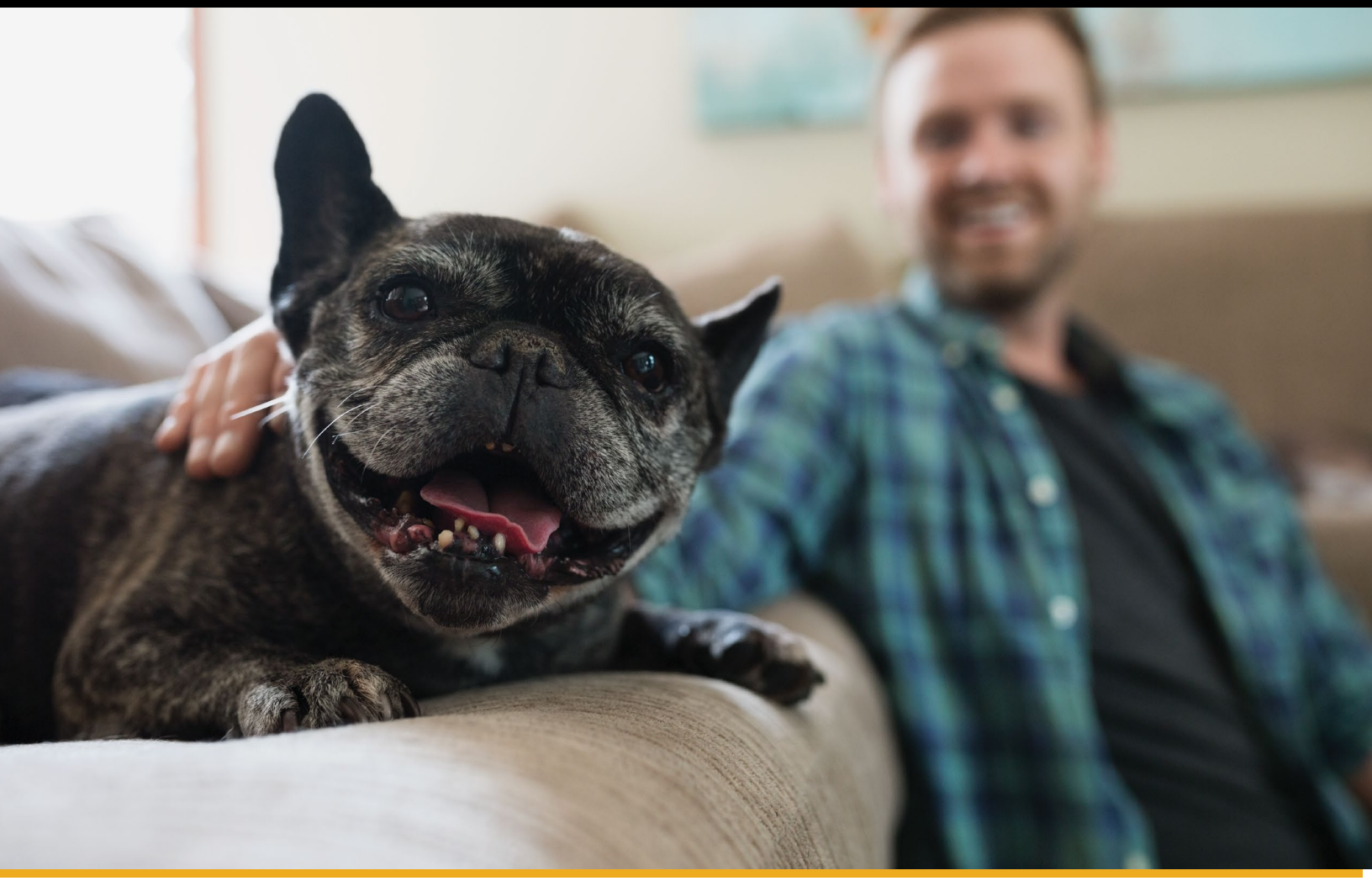
Creative acquisition:
There's no one-size-fits-all approach for buying cloud. Agencies should run a pilot program first to get an educated guess on the features they'll want and their associated costs. Then, acquisition teams should work with IT and security to put the proper services in place and craft usage guidelines.

Employee training:
The workforce needs to understand how cloud impacts them. While cloud is most important for security, contracting and IT professionals, all employees should know the basics of what cloud is and how it will change their jobs.

Modern security:
Securing the cloud requires collaboration among contracting, IT and security staff. By laying out clear and sustainable terms and conditions, agencies can ensure responsibilities are divvied up well, and by training employees, agencies can implement modern security practices, including authentication and encryption.

Working like a dog to build your enterprise cloud?

Knowing your data is safe gives everyone a good feeling.



Keep your head in the clouds and your paws on the ground. SAP has built solutions for government and regulated customers. A cloud portfolio of capabilities — all designed to support your unique security requirements in the cloud.

To learn more visit:
sap.com/regulated

THE BEST RUN SAP

INDUSTRY SPOTLIGHT

Making the Move to Cloud Comfortable

An interview with Guru Sarma, Federal Cloud Director, SAP

Moving to the cloud may be necessary, but that doesn't mean it's easy for agencies, which have to train their workforces, undergo lengthy acquisitions and enter into entirely different IT environments.

The transition, and all that goes into it, can be draining, so easy wins and time-saving opportunities are big pluses when possible.

"The ease of work is as important as other aspects," Guru Sarma, Federal Cloud Director at SAP, said in a recent interview with GovLoop. SAP can tailor cloud solutions to agencies' mission needs while ensuring compliance, security and privacy.

"Recently, we helped migrate the Navy's Enterprise Resource Planning (ERP) program that is responsible for managing more than half the Navy's finances to the SAP secure cloud environment, 10 months ahead of schedule," Sarma continued. "During the tech refresh, Navy ERP upgraded to SAP's high-performance analytic appliance (HANA) cloud-based platform. The transition enhanced resilience, visibility and survivability, in turn strengthening Navy readiness and supply chain visibility."

As agencies grapple with how to manage the change of cloud environments, they should look for solutions that can shoulder their workloads. By identifying privacy, security and implementation as windows of opportunity, agencies can advance and improve their cloud journeys.

1. Privacy

Privacy starts at the data layer. And here, there are several important questions to ask. First, what type of cloud is best for agencies? And second, who is responsible for cloud security?

To answer the first question, agencies have several options. In some cases, a FedRAMP-approved out-of-the-box software option will do just fine – as it's the cheapest and easiest. Sarma noted that government clouds are more secure, because of stricter controls, than private sector equivalents.

"With respect to the cloud security controls that are required for federal agencies, it is significantly different from commercial customers," Sarma said.

However, when agencies still worry about overall access, in addition to protecting data, they can install their own private clouds that run in vendor data centers. These private clouds are kept physically separate and have agency tools attached, so agencies have full control.

After deciding on the right cloud model, agencies must enforce the segregation of duties. This means that someone at the data level should not be able to pair the information with identifiers or have access to accounts. Otherwise, privacy could be compromised.

2. Security

The default agreement for agencies is an authority to operate (ATO) contract reached with vendors. ATOs signify that security is set and authorizes an IT system or product to operate on government networks.

The trouble is that too often, these ATOs can take months or years to finalize. When agencies realize that cloud is necessary, they might not be able to wait that long.

Therefore, federal agencies should take advantage of FedRAMP authorizations, which assign a security level for cloud providers through a central governmental office. FedRAMP was designed to do the painstaking work of providing provisional authorizations to vendors so agencies don't need to perform duplicative work.

Moreover, agencies should search for cloud solutions that let them carry over security controls from their pre-cloud environments. That way, instead of tearing down existing operations and starting from scratch, agencies can have the cloud accommodate the same security measures that staff and employees are familiar with. These can complement new security capabilities that are available in the cloud.

3. Implementation

Although procurement processes can still take a considerable amount of time even if agencies use FedRAMP, the hiatus should not be spent in limbo. Agencies should look for authority to test (ATT) agreements to precede the actual ATO.

With ATTs in place, agencies can begin pilots and testing before signing a contract. That way, they'll figure out all the quirks and nuances before officially launching the cloud.

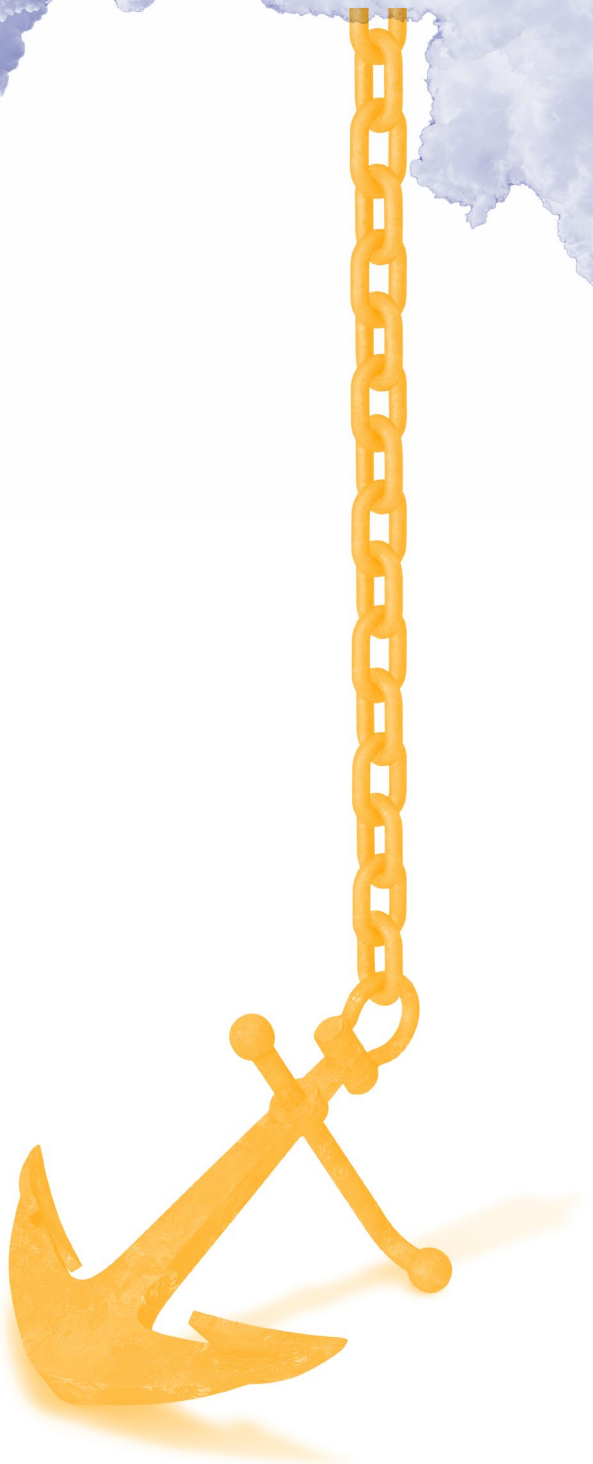
"They are able to get their ATO completed so that these activities are ready to go at the right moment," Sarma said.

Conclusion

Cloud is truly an anchor for innovation that agencies and employees have every right to get excited about. But it's also only one leg of the race to be run in government IT.

To get to the finish line of cloud, there's a lot that agencies need to do first: Network access needs to be expanded; security, acquisition and processes need to be reevaluated; and the people whose jobs are touched need constant communication and education throughout.

Wielding the cloud as a people-based solution takes a truly collaborative effort, and your voice plays a big part in it. Whether your agency's cloud is crawling, walking or running, your knowledge, concerns and ideas can spur the technology forward so that it has a positive impact on government.



ABOUT GOVLOOP

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

THANK YOU

Thank you to Avaya, AWS, Cisco, CyberArk, Elastic, Pure Storage, Red Hat, SAP, ServiceNow and Snowflake for their support of this valuable resource for public sector professionals.

AUTHOR

Isaac Constans, Senior Staff Writer

DESIGNER

Jacob Hege, Junior Graphic Designer

1152 15th St. NW Suite 800
Washington, DC 20005
P: (202) 407-7421
F: (202) 407-7501
www.govloop.com
@GovLoop