A fresh look: Capitals in the Clouds

2021 Accenture and NASCIO Cloud Study

When the world shut down due to the COVID-19 pandemic, state government agencies still needed to work and deliver services to citizens. Governments simultaneously saw a dramatic increase in demand and had an urgent need to respond to an unprecedented number of unemployment claims and demands for state social and healthcare services. As states around the country responded, they accelerated the move to remote and hybrid workforces, digital services and elastic cloud solutions, leveraging new funding sources and distributing financial relief, building new programs and establishing new operating models.

From this experience, two things became clear:

- Digital is more important than ever
- States need to be prepared to rapidly adapt their capacity to meet surges in demand

The cloud can be a tool to achieve both objectives. Globally, 57 percent of public sector leaders feel that accelerating cloud adoption is business critical, and 83 percent feel that it is essential to fuel innovation and enable new business models.[1]

This first biennial Accenture-NASCIO Cloud Study is intended to be a reference to help state governments better understand the current state of cloud in the public sector. It provides an overview of how states are transitioning to cloud and what challenges and opportunities exist today. The report is divided into three distinct sections.

1 The state of the industry

This section provides an overview of the cloud marketplace and is intended to reflect upon the past, the current state and the future of this marketplace. This is included because an understanding of the ongoing evolution of this marketplace may be critical to shaping a state government organization's cloud modernization strategy.

2 Key findings of state CIOs

This section provides an overview of the aggregated cloud survey results that were submitted by 35 states in May of 2021. This will help state government organizations understand where their individual cloud adoption strategy is relative to the rest of the states.

3 Pathways to progress

This section provides information about cloud maturity ratings and how those ratings are correlated to possible actions that a state government organization can consider. This report is accompanied by a maturity tool that states can use to measure their current cloud capabilities and correlate that measurement to possible actions reflected throughout the report that are tied to the maturity tool results. This is intended to allow states to gauge their readiness for these actions based on corresponding scores provided in the report.

1

State of the industry

The cloud market has evolved significantly since the days when virtualization technology spawned the service delivery model. In the early 2000s, there were few software as a service (SaaS) and infrastructure as a service (IaaS) providers and there were virtually no platform as a service (PaaS) offerings in the marketplace. As the service delivery model grew in popularity, the quantity of new providers exploded significantly—the number of companies offering SaaS grew from 450 in 2000 to over 15,000 in 2020.[2]

As this market expansion occurred, underlying service definitions in the form of contractual terms and conditions spread quickly with little standardization and vastly dissimilar service commitments, security capabilities, service levels, data ownership and customer protections. This made consumption of many such cloud services a “buyer beware” market. The different service categories remained siloed with distinct differences between SaaS, IaaS and PaaS. As the market matured, and large providers acquired small providers, the quantity of providers declined while strategic acquisitions allowed the catalog of services to expand.

As more organizations moved to the cloud, primarily driven by the private sector, the model resulted in frequent price reductions that were quite unique in the technology space. One cloud provider noted that their price dropped 67 times between 2006 and 2018.[3] As the cloud marketplace continues to evolve, the silos between these service categories are blurring and traditional sourcing for technology products are changing significantly. For example, the leading IaaS providers are now offering thousands of new services that meet the characteristics of IaaS, SaaS and PaaS from a single contract with a single provider. Traditional commercial off-the-shelf (COTS) providers are being acquired by cloud service providers (CSPs) and their packages added to the CSPs’ feature catalog.

Today, globally, cloud has gone mainstream. Underlying contractual terms and commitments have standardized. Government cloud environments are structured to satisfy the unique requirements that government organizations have related to resource access, stricter regulatory requirements and tightened service commitments.

Most industry observers agree that between 80 to 90 percent of enterprises have now adopted cloud services in some form. The COVID-19 crisis has accelerated what had already been a steady migration of IT workloads to the cloud over the past several years. Earlier concerns about data security, performance and the reliability of public cloud services have faded against the potential advantages of cost savings, security, identity management, scalability and efficiencies offered by cloud.

Worldwide across all industries, currently about three-quarters of cloud deployments are hybrid (a combination of public and private cloud), and the vast majority of cloud adopters are using multiple public cloud providers.[4] With hybrid cloud and multiple public cloud providers to manage, however, organizations are facing complexities that many did not expect in moving to cloud. There is now a need for an operating discipline to successfully manage the emerging enterprise cloud portfolio.

State governments are relatively new to the cloud market. The first mention of cloud services appeared on the NASCIO State CIO Top Ten priorities list in 2010. The increase in cloud adoption right before and during the pandemic has highlighted some growing pains as state leaders adapt to new operating models.

One immediate growing pain in the market is the budgeting and procurement process state leaders go through to acquire cloud services. Many states still lean on annual CapEx spending procedures to budget their cloud spending. This current, predominant budgeting process also affects procurement efforts and does not enable the necessary flexibility to properly utilize cloud services. This is a two-way street, though, and CSPs do not fully understand the nuance of government needs and requirements. This creates inefficiencies in what services are provided and which services are utilized. While there are growing pains for state governments and CSPs in this newer market, these known pains can be alleviated with greater cooperation.

The federal government, in response to early federal agency cloud adoption with poor outcomes and cloud sprawl, created the FedRAMP certification process. This is a fairly mature process in which most cloud providers in the federal marketplace participate. FedRAMP is a detailed certification process that cloud providers must complete in order to compete for contracts with federal agencies. Many states now seek this same level of certification as a criterion when considering cloud service providers. A very recent development is the new StateRAMP membership association and its certification process. While not affiliated with FedRAMP, StateRAMP acts as a similar certification method. StateRAMP will grant cloud providers that already have FedRAMP certification an equivalent StateRAMP certification and allow cloud providers that are not seeking a FedRAMP certification to become StateRAMP certified. The reciprocal does not happen, but this may allow select cloud providers that only wish to offer service to state and local government to gain a "certification" status within the markets they serve.

While the development of marketplaces, either through CSPs or FedRAMP and StateRAMP, have their benefits, the reliance on certificates can hinder agility and the pace of digital transformation. Some states, like Texas and Arizona, are seeking to resolve this issue by creating marketplaces so leaders within the state can easily find reputable, secure solutions. Additionally, under the National Association of State Procurement Officials (NASPO) ValuePoint cooperative contracts for cloud solutions, states have access to a portfolio of providers.

These efforts provide state leaders with greater transparency into pricing, solutions delivered and timetables that make it easier to find and implement cloud solutions. If states can utilize these marketplaces and employ new and more effective procurement processes, greater and faster digital transformation is possible.

Challenges persist and future innovations in procurement processes and vetting of CSPs can be anticipated to solve these issues.

Native cloud features continue to expand at a rapid pace in the public cloud; however, the government cloud environment, due to its more restrictive requirements, does not introduce new feature functionality at the same pace as the private sector.

New cloud service capabilities are also proliferating. New cloud broker services exist, new cloud access service brokers abound and new functional niche cloud providers appear regularly. The expanding number of services and interdependencies among these services add complexity state governments must address through a new discipline for managing and operating an enterprise-wide cloud portfolio that can deliver needed government as a service.

The industry has limited mandatory regulatory oversight, despite voluntary adherence to select regulatory frameworks, such as HIPAA, FERPA, CJIS and IRS 1075 certification processes. For some risk adverse organizations this can pose a challenge. Many potential CSPs may not be candidates for state governments that rely on the aforementioned requirement and certification processes states employ as part of their risk management discipline.

2

Key findings from state CIOs

In this broader context, we sought to understand the state CIO perspective on cloud transformation. We surveyed CIOs with the goal of better understanding the true state of states in relation to cloud.

State CIOs have coalesced on several key opportunities to be achieved from cloud adoption, including cost savings, flexibility and scalability, security and improved experiences for the residents of their state.

What are the major opportunities regarding future cloud strategies for state government?

But despite years of investment, most government organizations still have no more than 20 percent of their workloads in the cloud. What's more, research shows that nearly two-thirds of organizations are dissatisfied with the results to date from their cloud initiatives.[5]

It is clear that migration to the cloud does not automatically result in these benefits. New operating models must be implemented to fully take advantage of the cloud to secure these benefits. For example:

- Migrating to the cloud often allows organizations to capture cost savings and shifts an organization from the challenging capital IT budgeting and planning cycle to a model of ongoing IT operating expenses. However, new governance models and financial processes must be implemented to "manage the meter," realize savings and ensure that organizations do not incur unexpected usage costs.
- The best cloud providers provide cloud IT security in conformance with leading security frameworks, policies and standards. However, cloud providers limit their focus to security of the cloud, while cloud customers are still required to provide security for their resources they elect to place in the cloud. State organizations will still be required to understand how to architect and configure security within their cloud environments.
- Clouds are inherently more scalable and flexible than other solution delivery models, but solution architectures can span multiple non-cloud and cloud environments and may require a re-design to take advantage of cloud elasticity.
- The agility that the cloud service model offers may not be fully realized if organizations do not transform themselves by adopting an agile culture that includes procurement, legal, program teams and IT.
- States are still responsible for software asset management, contract and license management even though the software resides in a commercial cloud.

Hybrid cloud

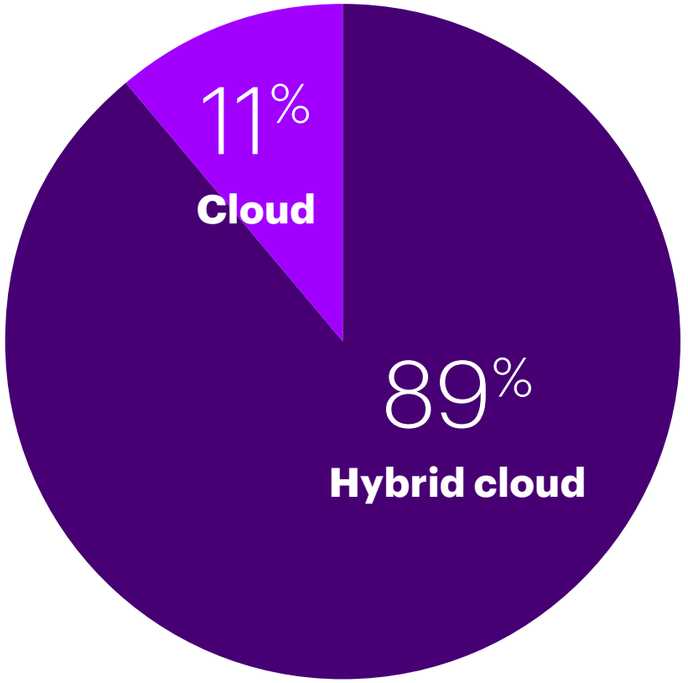
State CIOs are clear on what they are working towards. Eighty-nine percent of states reported that hybrid cloud is their ideal cloud state. A hybrid cloud is typically defined as a composition of two or more clouds (with at least one public and one private) that remain unique entities but are bound together, enabling application and data portability.

Organizations prefer the flexibility they have when placing workloads in a hybrid cloud model. The private cloud environment allows them to leverage their existing investment in private computing infrastructure and hosting workloads that have unique regulatory, security or performance requirements. At the same time, they use the public cloud environment to deploy:

- Elastic workloads that must rapidly and cost efficiently scale
- Specialized workloads that require cloud native capabilities, such as artificial intelligence, machine learning and edge computing

A mature hybrid cloud allows these environments to be managed holistically through a single interface and set of processes, even allowing workloads to seamlessly transition across environments as needed.

What's your state's desired end-state technical operating environment?



Cloud definition

The definition of cloud varies, with marked differences in what states consider "the cloud." One state said they had no common definition of cloud across the enterprise. Twenty percent considered off-premise computing to be the cloud, while 40 percent said they used the NIST definition of cloud.

For purposes of this survey the NIST definition[6] is used, however a common definition and shared language of what is meant by cloud should be more widely established.

In recent years, while the IaaS market has consolidated around a handful of large providers, the SaaS market has exploded: Estimates put the total number of SaaS providers at over 15,000 in 2020.[7]

CIOs reported a range of cloud service providers, with an average of nearly 22 providers per state. Some states reported 99 different providers. This expansion of cloud providers means that setting an effective enterprise-wide cloud portfolio management strategy is more important than ever, and states must ensure that they are aligned on what functions are handled by each provider and what obligations remain as the responsibility of the state government customer.

NIST definition of Cloud computing: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

How states are defining cloud

"On-demand availability of computing resources without requiring active management by the user, whether on-premise or remotely."

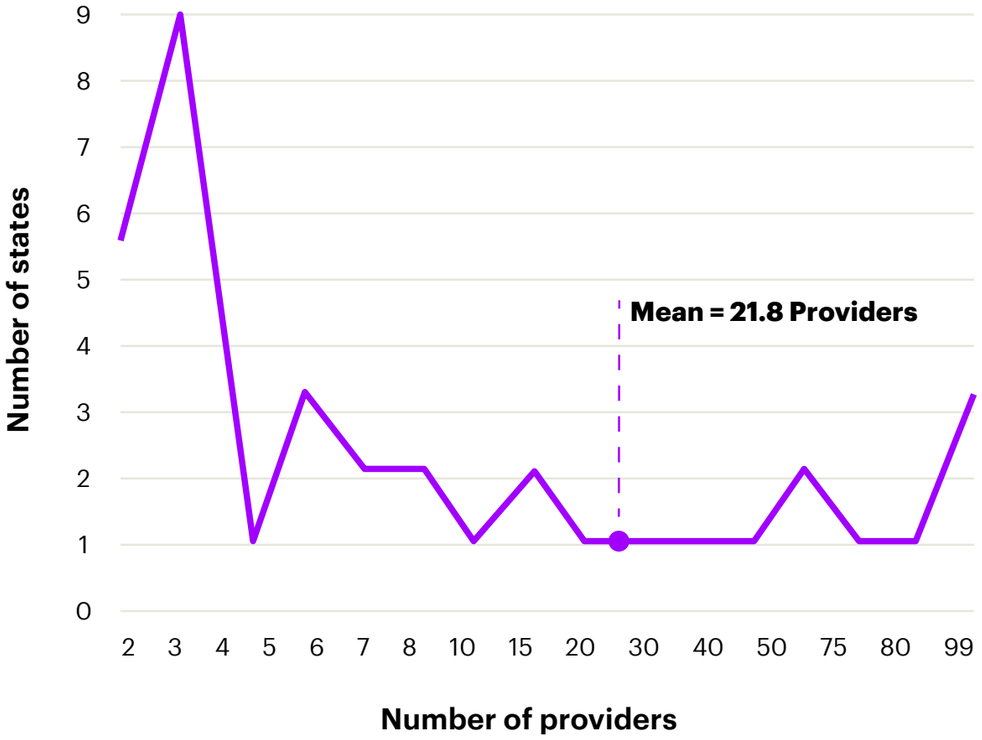
"Workloads hosted in someone else's data center, on someone else's servers, that can be fully configured through software."

"A computing practice where scalable and adaptable IT-enabled capabilities are delivered as a service to external customers using cloud-based solutions. Cloud services can be delivered by a third-party cloud service provider (CSP), or internally through the establishment of state owned services and infrastructure."

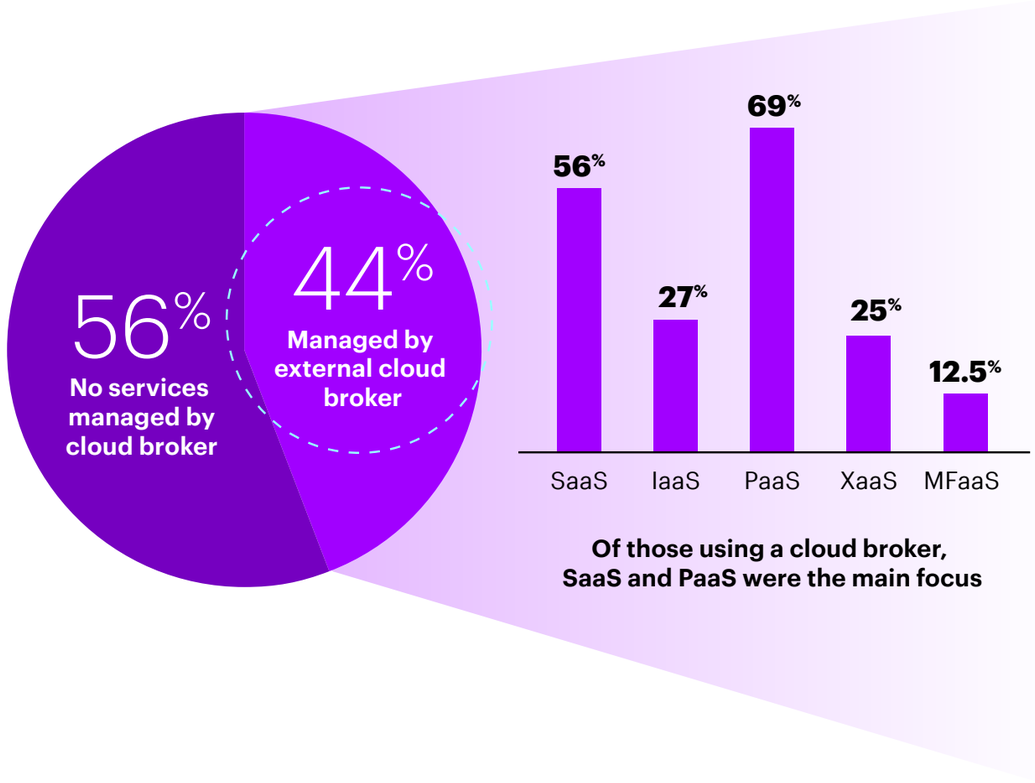
"We use the NIST definition."

With such a large number of cloud service providers, some states have turned to an external partner to help manage their services. Forty-four percent of states report the use of an external cloud broker, with these services most frequently being used for SaaS and PaaS.

How many different cloud service providers are in your state?



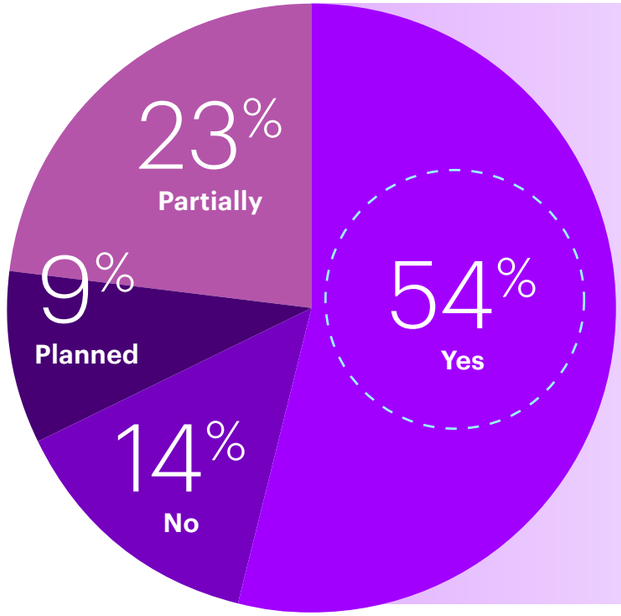
Are any cloud services managed by an external broker?



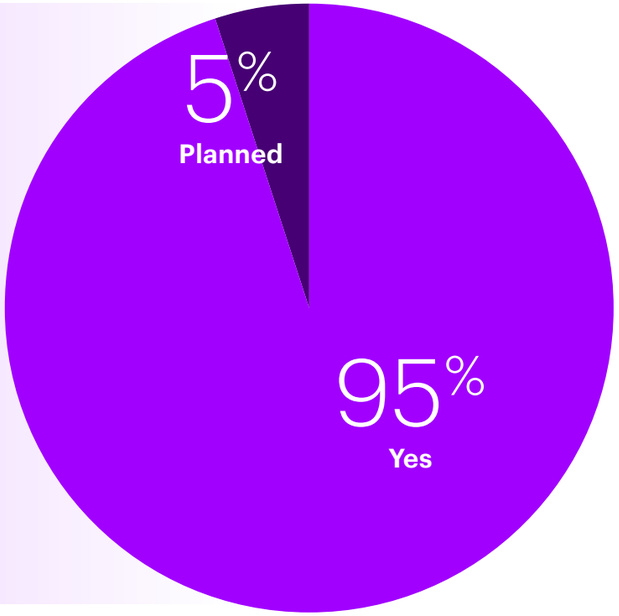
Cloud change management

Only 54 percent of states report having a cloud IT change management strategy in place. Of those states, 95 percent report that it is integrated with the state's IT change management plan. To effectively manage the increasing complexity of cloud environments, an IT change management process and governance structure is critically important to control the cloud environment, reduce operational and security risk and maintain service delivery agility.

Do you have an established cloud change management process?



Is it integrated with your state's change management?



Cloud barriers

The journey to cloud is not without storms. State CIOs identified key barriers to this transition as:

- Budget and financial
- Cybersecurity management
- Procurement
- Workforce

What do you see as a major challenge regarding future cloud strategies for state government?

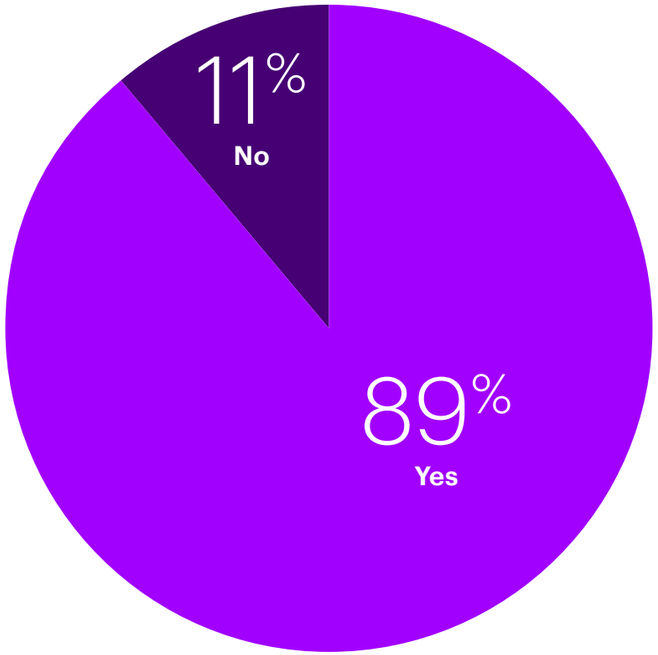
What are cloud service options lacking today?

CIOs indicated that certain functionalities were missing from vendors' cloud offerings. Integration, pricing and transparency topped the list of areas that can be improved by cloud service providers.

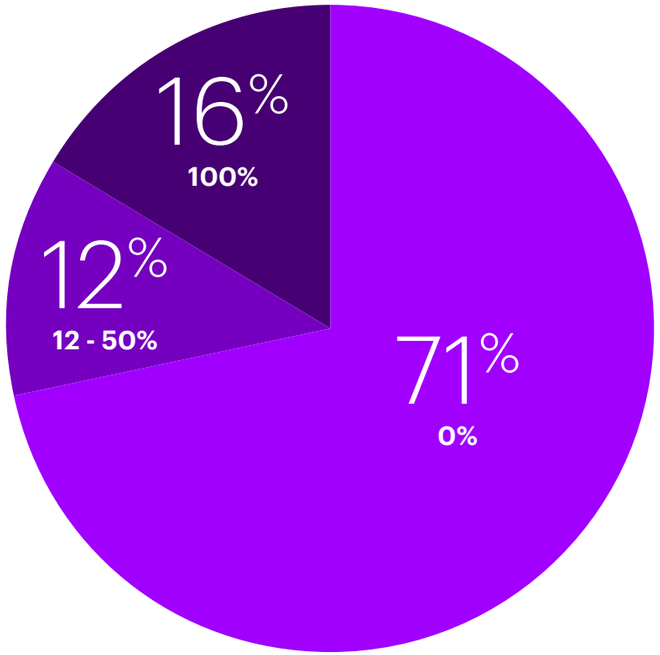
Technical strategy is evolving

The switch from mainframe on-premise to a mainframe as a service (MFaaS) is slow—as nearly all states, 89 percent, report that they have a mainframe computer and 71 percent indicate that they have not moved any applications to MFaaS. The primary driver for moving to MFaaS is cost savings. MFaaS will likely be a large part of modernization strategies moving forward.

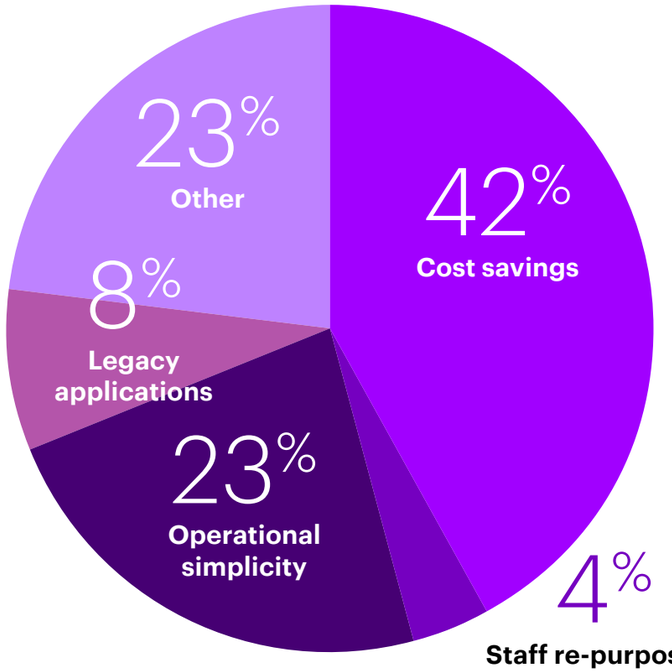
Does your state currently have a mainframe computer?



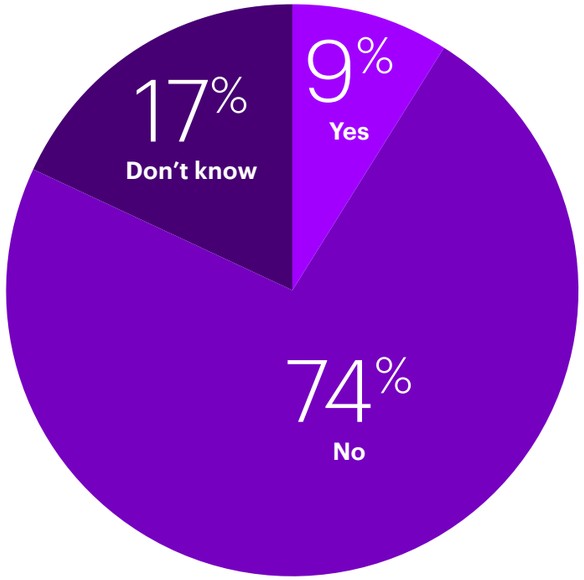
What percentage of mainframe applications have been moved, if any, to MFaaS?



What is the primary driver for considering MFaaS?

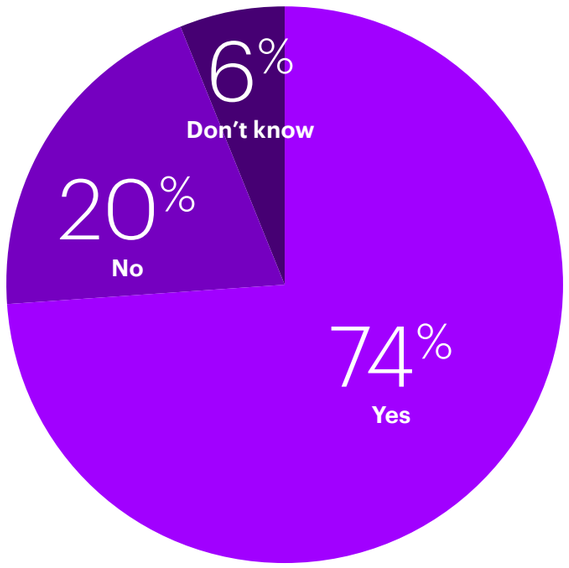


Does your state currently require possession of the title (ownership rights) to all computing assets?



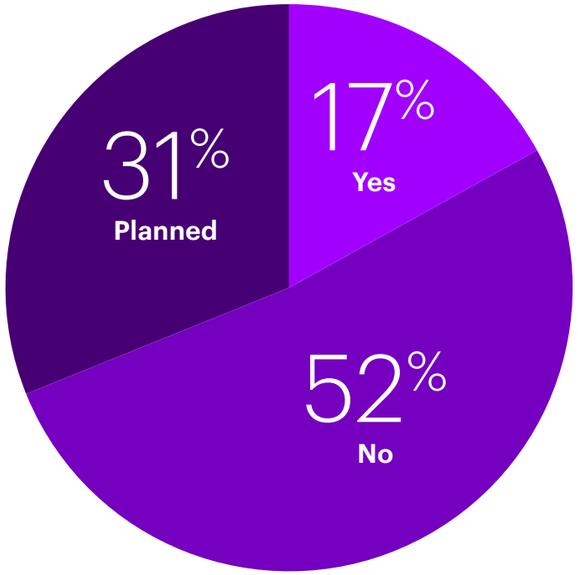
Over 74 percent report that they do not require ownership rights to all computing assets. This is an important consideration as states plan to incorporate cloud services in their modernization strategies given the subscription nature of cloud services. For states that require titled possession of computing assets, extra focus is needed as there will be a legal hurdle to overcome when building a modernization strategy that includes cloud.

Do any of your state's systems still use hard-coded IP addressing vs. DNA?



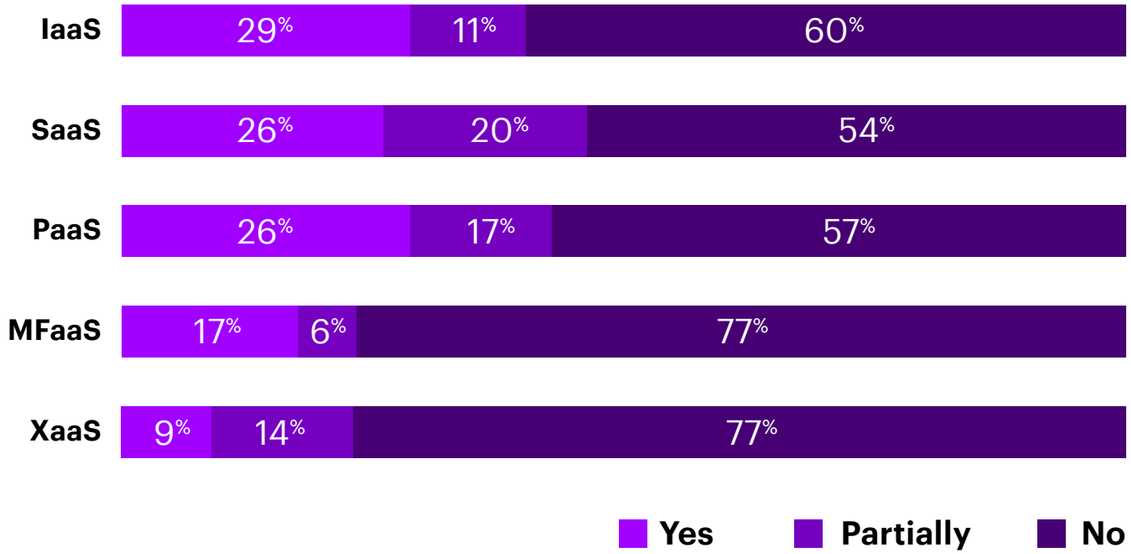
Seventy-four percent of states report that they are still using hard-coded IP addresses for at least some systems, which creates a significant hurdle for migrating applications to cloud environments. This can be a challenging resource drain for development teams to cloud-enable workloads in advance of migration. This will require significant planning to adopt the most effective application cloud-enablement strategy, whether it be addressed by coding, refactoring, containerization or other means.

Does your state have a container strategy?



Only 17 percent of states report having a container strategy in place, while 31 percent have a container strategy planned. A containerization strategy will be critical for migrating workloads across clouds in a hybrid cloud or multi-cloud architecture. When workloads can be migrated across clouds, it allows organizations to avoid being locked into a single cloud provider.

Is your service desk integrated with your cloud service provider's (CSP) services?



A majority of states report that their service desk is not integrated with their cloud service providers' services. Increasing this integration will be key to long term success, allowing for real-time problem solving and eliminating a gap that exists when providers aren't fully integrated. SaaS and PaaS categories seem to be further along in the integration process, with 46 percent and 43 percent of states reporting that they are at least partially integrated.

Just over half of states (57%) have a statewide application inventory, fewer states (40%) have an application risk assessment and still fewer (34%) report a legacy application assessment. The key to understanding what can be migrated to cloud, and in what order, is understanding the applications in the current application portfolio, their characteristics and their associated business priorities and risks. While this may be harder in a decentralized environment, it is important for all states to establish a baseline inventory and assessment. This initial effort is essential to a successful enterprise cloud computing strategy.

Possible Actions:

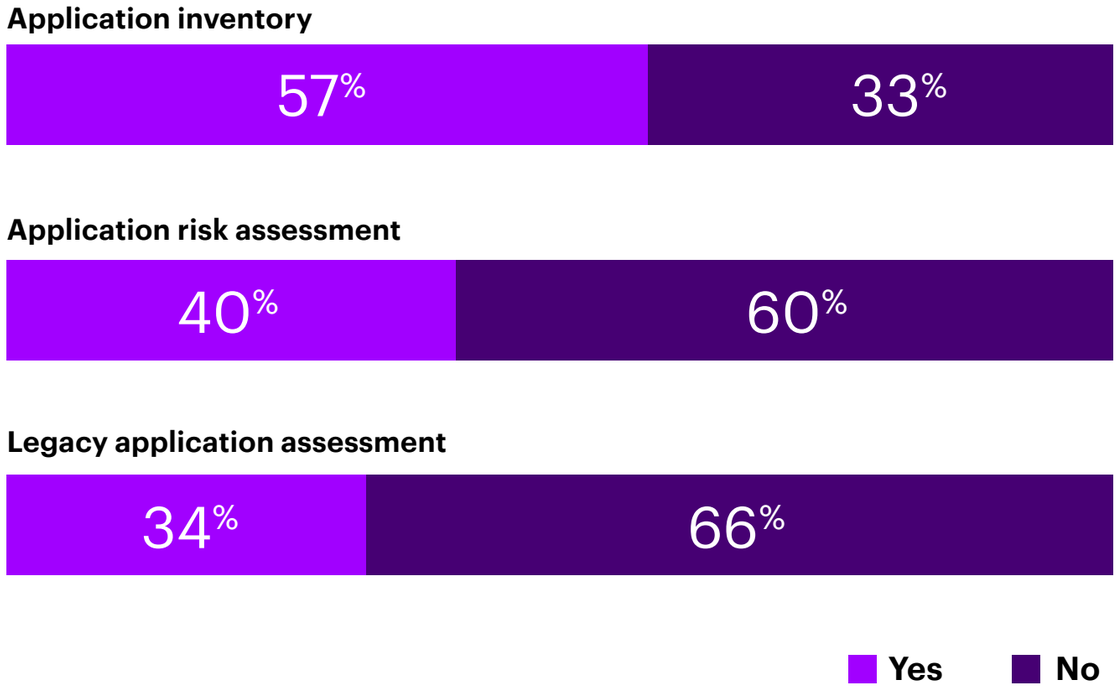
Start the switch to mainframe as a service. (**Maturity level 3**)

Evaluate the risks around ownership. (**Maturity level 2**)

Integrate the service desk. (**Maturity level 2**)

Inventory all applications. (**Maturity level 1**)

Do you have up to date, statewide versions of the following?

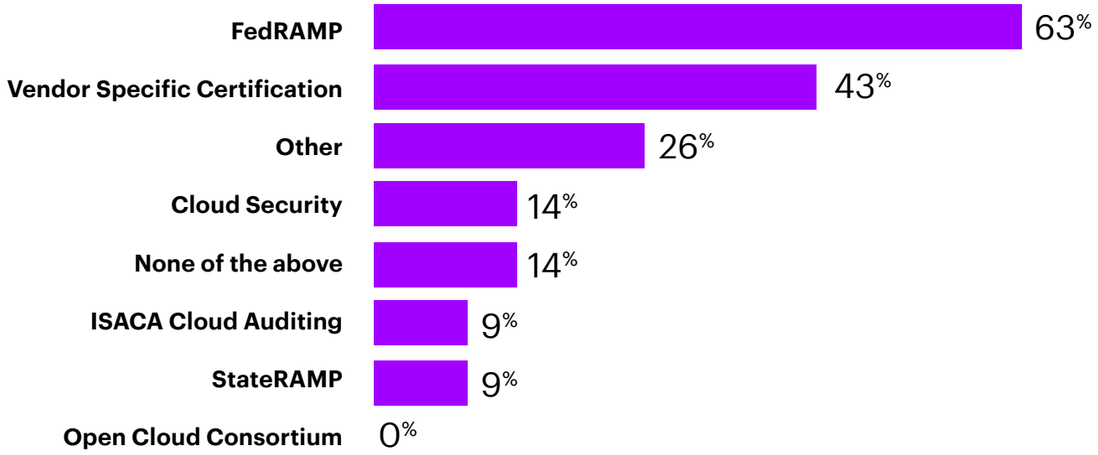


Throughout this report we provide the maturity level associated with each action. A maturity tool accompanies this report and states can use this tool to measure their current cloud capabilities. By completing this measurement, states can determine if the action is appropriate for their current state.

Cloud and Cybersecurity

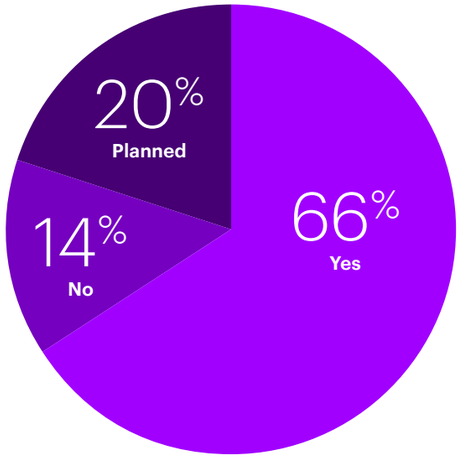
States indicated cybersecurity management as a barrier to cloud adoption, and rightfully so, as ad hoc adoption of the cloud can lead to security risks. A recent cloud security report found that 66 percent of survey respondents feel that traditional security solutions do not work or have limited functionality in the cloud.[8] Cloud native cybersecurity measures can help to mitigate some of the risk.

Which of the following cloud certification/standards programs does your state require?

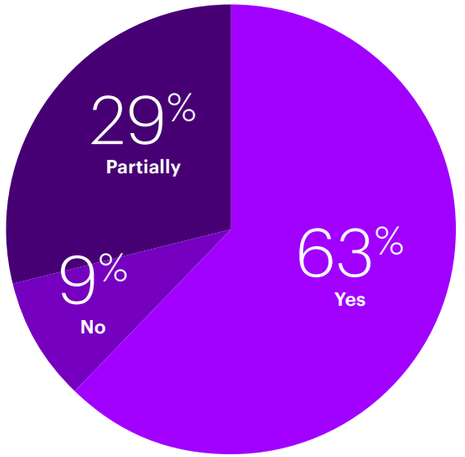


Sixty-three percent of states report that they currently depend upon FedRamp certification, however some states are starting the pivot to employ StateRamp, with nine percent of states incorporating StateRamp certification. Forty-three percent utilize vendor specific cloud certifications.

Does your state have a process for managing cloud-related privileged permissions?



Are cloud-related logins and access activities monitored?



Only 66 percent of states indicated they had a process for managing cloud related privileged permission and 63 percent said cloud access related activities are monitored.

Only 51 percent of states reported using multifactor authentication for IaaS, while 46 percent indicated they were using it for SaaS and PaaS. The fewest states reported using it for MFaaS, where only 11 percent of states reported using it.

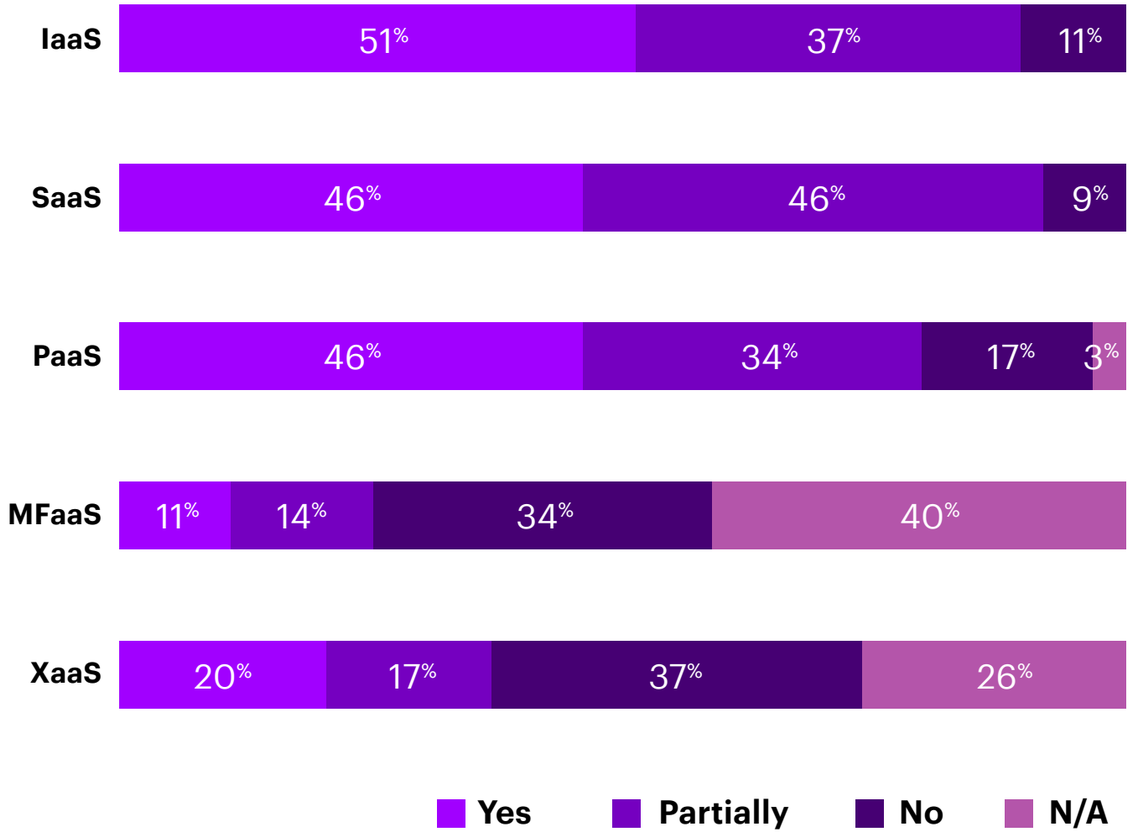
Possible Actions:

Incorporate state identity, credentialing and access management (SICAM) into cloud strategy. (**Maturity level 2**)

Incorporate end user cloud awareness education such as phishing, spearfishing, smishing and other threat profiles that can occur as a distributed workforce accesses cloud computing from non-centrally secured locations. (**Maturity level 2**)

Explore cloud native security offerings and meet with current security product owners to understand how their products align with cloud service providers. This could influence the selection of cloud partners and should be included as a necessary process step in cloud procurement operating discipline. (**Maturity level 2**)

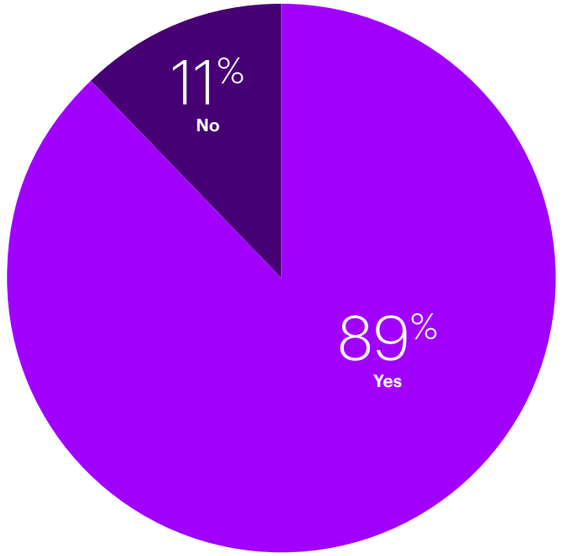
Is your state using multi-factor authentication for cloud services?



Budget and procurement

Nearly 90 percent of states report having documented and implemented unique procurement processes aligned to cloud solutions. Despite this response rate, procurement remains, at least anecdotally, an issue. States have not adapted to cloud procurement and further focus is needed on aligning terms and conditions that account for data portability and address data breaches.

Does your state have documented and implemented procurement processes for cloud?



Budget presents another challenge, with distinct differences between centralized and decentralized enterprises.

Sixty-three percent of states said they used usage or metered billing for cloud services, while 37 percent said that they utilized reserved billing and 34 percent utilized flat billing. Fifty-four percent of states preferred OpEx to CapEX.

The budget office still needs to evolve their model and has not kept up with the changing reality of cloud—budget procedures and standards set up to support the financing of capital expenditures are not flexible enough to support budgeting for cloud services. The future CIO will be buying services more than making capital expenditures and this should be considered as states expand financial governance. The financial risk for ad hoc adoption of cloud services without a plan can result in variable costs that can exceed a fixed budget.

While the flexibility and scalability of the OpEx model is one of the most attractive elements of the cloud service delivery model, it is also the biggest risk. As demand for services increases and decreases (with close monitoring of that consumption relative to the planned budget), a mature cloud organization will have controls in place that effectively match resources to that demand. There should be no surprises if the forecasting models used to create budgets for cloud services are effective. As appropriate, these forecasting models need to be reviewed and updated.

Possible actions:

Continue to evolve budgeting for the reality of cloud. (**Maturity level 2**)

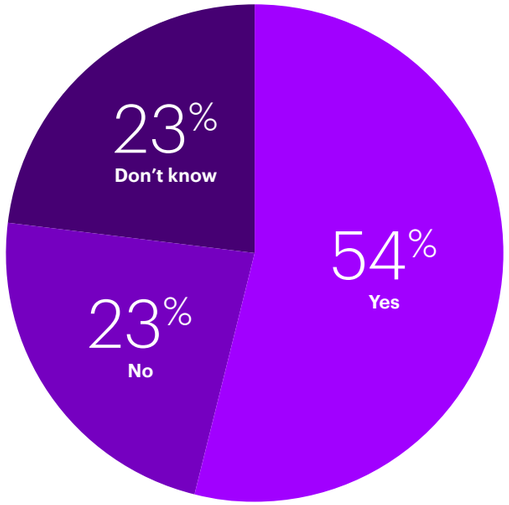
Work with policymakers to explore variable-based budgeting. (**Maturity level 3**)

Work with procurement officials to adopt agile procurement methods. (**Maturity level 2**)

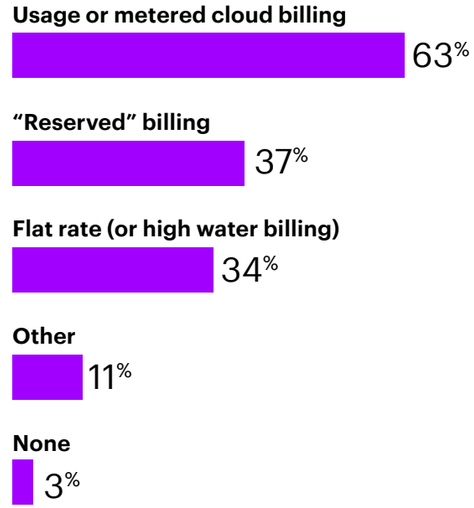
Build the business case for operational expense instead of capital expense for large IT projects. (**Maturity level 2**)

Adopt an incremental approach to IT projects that breaks a single big project into many smaller projects. (**Maturity level 2**)

Does your state budget office have a preference for OpEx over CapEx?



What type of cloud billing does your state use? (Multiple response)

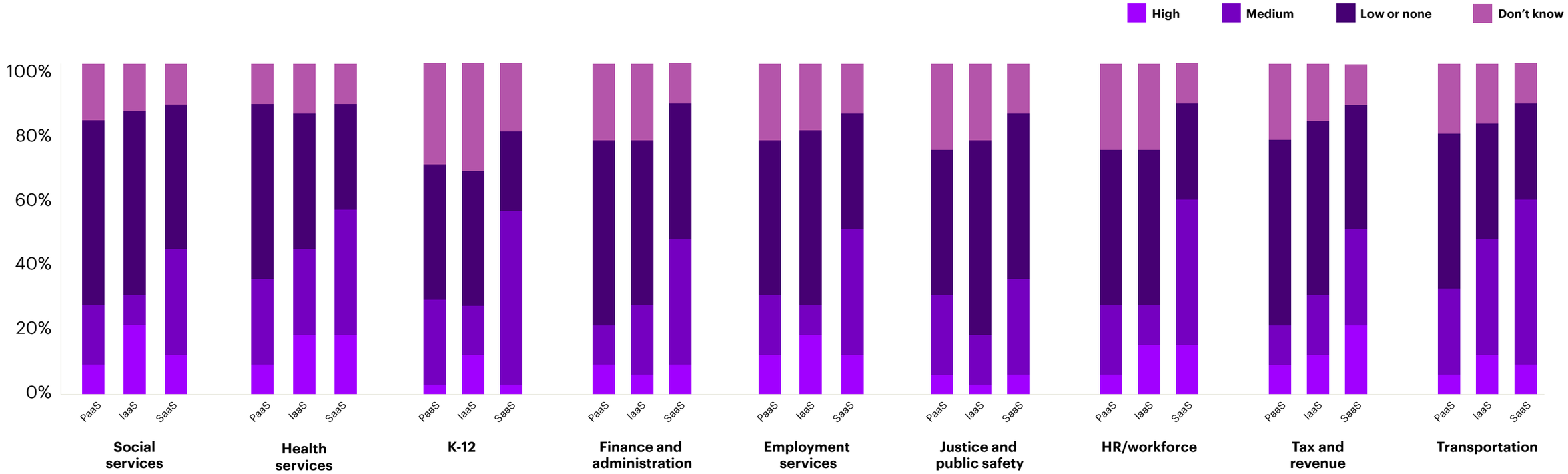


Function impacts cloud adoption

States reported that the adoption of cloud varies based on function. Areas that show increased adoption of cloud are more often areas that need scalability and responsiveness, such as social services, health services or employment services. Public safety and justice, both areas with more control parameters, have less uptake of cloud.

Across all functions, SaaS is more adopted than IaaS or PaaS.

How would you rate the level of adoption in the following agencies?



3

Pathways to progress

The specific goals, objectives and business strategies for modernization that are expected to embrace cloud computing as an enabling technology strategy are unique to any state organization. Despite having access to best practice resources, lessons learned resources and proof of concept resources, it remains incumbent upon each individual organization to chart their own unique course to assure an optimized cloud operation is realized.

The survey results that drove this report indicate that states are adopting cloud in a deliberate and cautious fashion. This leads to mixed results, as the cost savings, scalability and flexibility the cloud operating model provides are not being fully realized, while the more deliberate and cautious approach reduces risk. The trade-off between risk and benefit is not a new one for states. This balancing act occurs every day from a cybersecurity perspective, a political perspective and a fiduciary optics perspective.

Understanding where any specific state organization lies in a capability spectrum is a critical self-awareness to have when building a state strategy for modernizing to the cloud, whether selectively or entirely. Do states have the right resources in terms of people, process, technology and funding? Building a plan that assumes you do, when in fact you don't, will only waste valuable and typically limited resources and result in not realizing the benefits that the cloud model offers.

In order to help more consistently measure and understand the state organization's capabilities at a moment in time, a self-assessment tool is provided as a companion to this report. This tool will help rate the state organization's capability maturity in 40 key cloud controls.

The tool is used to rate each organization on a scale of zero to five, where zero indicates an organization has no capability for a particular control, up to five which indicates an organization's capabilities are highly optimized. The following recommended actions and goals that are tied to the self-assessment maturity scores. All actions are tagged with a number to indicate the maturity level for which the action is most likely appropriate.

Self-assessed maturity scale is 0 to 1:

- Evaluate SaaS solutions for a new application need that doesn't need to interface with existing application portfolio.
- Create a sandbox environment in an IaaS cloud environment and have your development team and operations team build and operate a test instance.
- Document your change management processes.

Self-assessed maturity scale is 1 to 2:

- Continue to build on earlier recommendations.
- Develop a formal change management plan for SaaS solutions in operation.
- Do a small proof of concept or pilot using a stand-alone workload to migrate to a cloud environment.
- Consider doing a lift and shift to IaaS for a small percentage of workloads.
- Develop a complete application portfolio.
- Develop an IT governance process.

Self-assessed maturity scale is 2 to 3:

- Continue to build on earlier recommendations.
- Integrate cloud service management with on-premise service management.
- Build a modernization strategy for prioritized workloads.
- Implement Dev/Sec/Ops processes.
- Develop a cloud center of excellence.
- Implement an agile culture.
- Expand governance structure to the enterprise.

Self-assessed maturity scale is 3 to 4:

- Perfect earlier recommendations.
- Implement self-service cloud orchestration portal.
- Expand on dev/sec/ops process to create full continuous integration and deployment pipelines.
- Create a cloud marketplace and service catalogue of complaint services to be used in continuous integration and deployment.
- Optimize existing cloud workloads using cloud native tools and features.

If the self-assessed maturity scale is 4 to 5—great work by you and your team! Share your story and help your peers learn.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 624,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Research

Accenture Research creates thought leadership about the most pressing business issues organizations face. Combining innovative research techniques, such as data science led analysis, with a deep understanding of industry and technology, our team of 300 researchers in 20 countries publish hundreds of reports, articles and points of view every year. Our thought-provoking research developed with world leading organizations helps our clients embrace change, create value, and deliver on the power of technology and human ingenuity. For more information, visit www.accenture.com/research.

About the research

This research is based on a survey of state government CIOs that was fielded in May 2021. The survey was sent to all NASCIO members and was completed by CIOs from 35 states. In-depth interviews were also carried out with state CIOs from seven states.

About the National Association of State Chief Information Officers

Founded in 1969, the National Association of State Chief Information Officers (NASCIO) represents state chief information officers (CIOs) and information technology (IT) executives and managers from the states, territories and District of Columbia. NASCIO's mission is to foster government excellence through quality business practices, information management and technology policy. NASCIO provides state CIOs and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. From national conferences to peer networking, research and publications, briefings and government affairs, NASCIO is the premier network and resource for state CIOs. For more information, visit www.NASCIO.org.

Authors and contributors

Todd Kimbrel, Jenny Brodie, Ryan Callison, Eric Sweden, Doug Robinson, Amy Glasscock, Douglas Chandler, Toms Bernhards Callahan, Rick Webb.

Thank you to the following states for their input, guidance and advice during the shaping of this report: Arizona, Georgia, Idaho, Maryland, Nebraska, Pennsylvania and Virginia.

Resources

[1] Public Services in the Cloud: A continuum of opportunity

[2] CardConnect.com, based on Crunchbase data.

[3] New Research from TSO Logic Shows AWS Costs GetLower Every Year

[4] Flexera 2021 State of the Cloud report.

[5] Hybrid Cloud: Enabling the rotation to the new

[6] The NIST Definition of Cloud Computing

[7] CardConnect, The Rise of Software as a Service (SaaS) June 16, 2020