Cloud Procurement for the Enterprise

Strategies to help government and education leaders optimize their cloud environments for today and tomorrow

While cloud adoption in government has accelerated in recent years — especially during the pandemic — the processes and tools needed to support this modernization have not kept pace. And even though governments have become more versed in procuring cloud technologies, there is a need for CIOs and procurement officials to develop enterprise roadmaps for modernization to ensure long-term success.

Today's IT environments include a combination of legacy and cloud systems, as well as solutions connecting the two. This combination of old, new and rapidly adopted systems brings with it a lot of risk for continuity in operations, according to William Sanders, Oracle's director of strategy and business development.

The task in front of state and local government IT leaders today is to develop an effective policy framework around cloud that enables expansion and optimization of the cloud-based transformation already underway.

Drawing from results from a survey of 128 government leaders conducted in April 2021 by the Center for Digital Government (CDG) and expert interviews, this paper outlines the key challenges governments face and offers strategies to plan, procure and secure cloud solutions in ways that serve rapidly evolving constituent needs.

About this Survey

The Center for Digital Government surveyed 128 state and local government leaders on cloud procurement topics in April 2021.

More than 60 percent of respondents hold positions in IT or administration and represent a broad range of functions, including public works, finance, law enforcement, health and human services, elected officials, emergency operations, environmental services, courts and agriculture.

"Speed is a theme we are hearing a lot — it is what we expect from our vendors and need from our contractors," says CDG Senior Fellow Dugan Petty, formerly Oregon's chief information officer and purchasing manager. "We cannot labor under old procurement processes any longer."

GOVERNMENT AND CLOUD

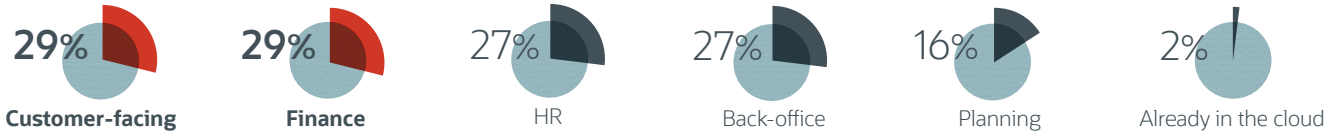
Government cloud adoption continues to accelerate. Just 14 percent of CDG survey respondents said cloud procurement is not a priority over the next 12 to 18 months.

"We have moved beyond the tipping point," says Petty.

Over the past year, survey participants moved or made plans to move a wide range of mission-critical applications to the cloud. These solutions run the gamut of government operations, including customer-facing services, finance, human resources and back-office applications (see chart, below).

Governments are also exploring a wide range of transformative and emerging technologies enabled by cloud environments, led by platforms to improve data sharing among systems and agencies. Other top priorities include artificial intelligence/machine learning (AI/ML); online chatbots; autonomous capabilities; open application

Have you moved or considered moving any of the following applications to cloud in the past 12 months?



A Cloud Glossary

Cloud services include data storage and computing power, but also cloud-hosted applications, networking solutions, APIs and other integrations, and database management and development tools.

Cloud service providers (CSPs) are companies offering cloud-based platforms, infrastructure, applications or storage services.

Cloud brokers or cloud service brokerages (CSBs) act as an intermediary between customers and one or more cloud service providers, helping manage relationships and ensure the use, performance and delivery of cloud services.

Service level agreements (SLAs) define expectations in vendor contracts and agreements, including the metrics by which service is measured (availability/uptime, performance, etc.) and remedies or penalties when those levels are not met.

System integrators (SIs) help customers implement, plan, coordinate, test, upgrade and maintain computing operations, including connecting multiple systems and automating repetitive functions.

As-a-service models refer to procuring technology needs as a recurrent operating expense vs. capital expenditures. Models include software-as-a-service (SaaS) for cloud-hosted applications; infrastructure-as-a-service (IaaS) for cloud-based data storage, servers and networking; security-as-a-service (SECaaS) for outsourced cybersecurity monitoring and response; and platform-as-a-service (PaaS) for integrated cloud-based infrastructure and development tools.

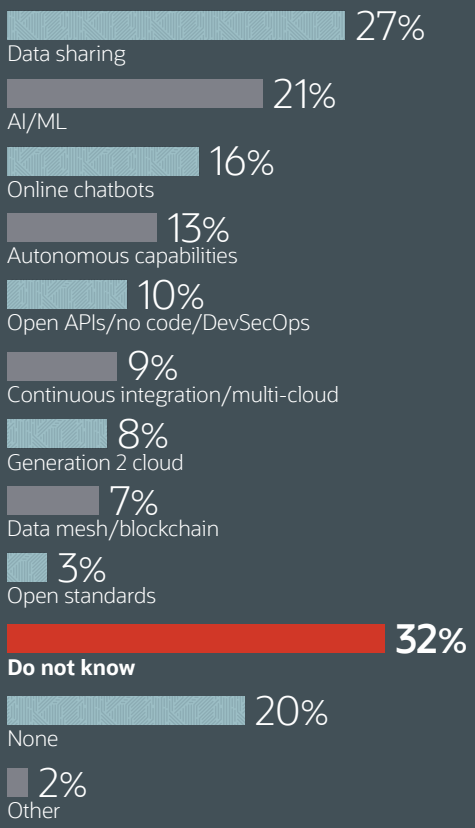
Workload is a description of the time and computing resources required by an application, function or task — typically a specific program or service running in the cloud or being considered for cloud migration.

programming interfaces (APIs); and a range of development methodologies such as DevSecOps, no-code environments, and continuous integration and delivery. Notably, one in five CDG survey respondents (20 percent) — and only seven percent of all state-level respondents — reported no plans to implement these cutting-edge technologies.

At the same time, government leaders' understanding of cloud priorities is becoming more granular and sophisticated. Nearly four in 10 respondents familiar with their organization's cloud priorities are focused on revising governance policies (39 percent) and optimizing existing cloud services (38 percent). Thirty percent of respondents plan to increase their use of software-as-a-service (SaaS) applications and 28 percent plan to convert to platform-as-a-service (PaaS) to streamline application development. More than one-quarter (26 percent) are planning to revise their overall cloud strategy, while others are focusing on managing cloud costs and cloud broker services (see chart, on page 5). However, governments still face familiar challenges to cloud adoption. Survey respondents cited cost, security concerns and a lack of trained staff as their top three barriers, followed by the need for cloud governance, constraints among departments, data compliance issues and concerns involving business continuity (see chart, on page 7).

Growing familiarity with cloud has mitigated some of these concerns. For

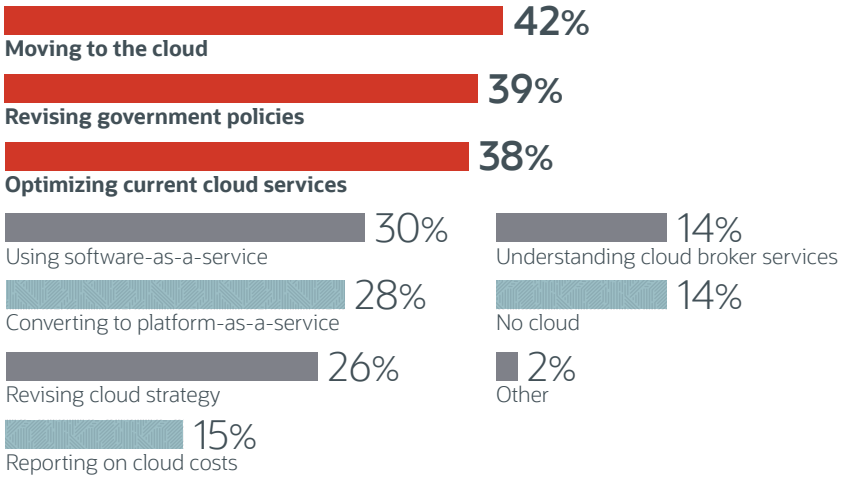
Have you considered any of the following transformative or emerging cloud technologies in the past 12 months?



example, only half as many survey respondents cited data compliance issues as a barrier in the 2021 survey as in a similar survey in 2017, and concerns about security fell by 15 percent during that period. Barriers involving constraints between departments, lack of trained staff and regulatory frameworks also fell over the past four years.

Even so, governments must still address these barriers in coordinated ways. "One of the things that is absolutely critical is that there is a shared understanding of what a government entity is attempting to accomplish with a given cloud procurement," Petty says.

What are your organization's top three priorities for cloud procurement in the next 12-18 months?*



** Respondents were asked to select their top three priorities from a list of 10.*

PRIORITY AREAS OF FOCUS

Addressing the key barriers to cloud migration requires a coordinated approach to not just procurement, but also managing costs, addressing security and developing an enterprise strategy that maximizes cloud assets.

Modernizing Procurement

Governments initially struggled to shift procurement practices to reflect the reality of the cloud. But now, more government organizations are making the transition from capital to operational expenses that cloud-based services require. More than 60 percent of CDG survey respondents reported being very or somewhat familiar with their organization's cloud procurement processes.

However, fewer government organizations have developed consistent frameworks and guidelines for procuring cloud services. According to the CDG survey, just one-quarter (24 percent) of IT leaders reported having such systems in place, although another 36 percent said they are currently developing them.

Top Strategies:

Develop cross-functional working groups. Two-thirds of survey respondents said their enterprise IT department oversees cloud procurement, often — but not always — in cooperation with their procurement and finance departments. It is also important to include business owners in the procurement process. Oracle's Sanders suggests developing cross-functional working groups to ensure governments "are really getting the best technology and the best providers."

Engage vendors early in the process. Better procurement involves developing better requirements. One important strategy entails having deep conversations with vendors about business needs and cloud capabilities in advance of the traditional freeze in communications during the RFP process, according to Petty. "If vendors can't understand what the background is and what the challenges are, then they are going into procurement with one hand tied behind their back," he says. Working groups can host forums or other collaborative information-sharing venues with multiple vendors before developing proposals.

"It should be an iterative process," Petty says. "The business problem and challenge should look a little bit different after a strong dialogue, and then you can develop a procurement strategy."

Evaluate vendors, not just proposals. More than one-quarter (27 percent) of survey respondents reported vendor performance as a challenge, with similar numbers reporting issues with visibility into vendor processes (22 percent) and service level agreements (19 percent).

As a result, more than three-quarters of CDG survey respondents (84 percent) either have or are developing procedures to evaluate cloud providers. Governments need to focus on ensuring the provider's area of expertise — applications or infrastructure — meets the needs of the specific modernization project. More traditional criteria for evaluating vendors, including longevity and stability, also hold true in the cloud environment.

"All three are important, and all three need to work together," he says. "Who cares if your system's available if you can't do anything? And if you have high availability architecture to deliver services, it has to be manageable."

Governments should also ensure their own business objectives are reflected in SLAs — which requires business owners to be involved. "Sometimes SLAs are measuring the things vendors traditionally measure and may not actually capture the actual performance that the government or business unit needs," Petty says. "Understanding the business problem will prepare the government for negotiation."

"One of the things that is absolutely critical is that there is a shared understanding of what a government entity is attempting to accomplish with a given cloud procurement."

— Dugan Petty, Senior Fellow, Center for Digital Government

It is also important to consult with a vendor's other government customers to get a handle on real-world operating costs, according to Glenda Sakati, Oracle's group director of government resell programs. "Customer references, not just expected cost projections, are key to the procurement process," she says.

Refine service level agreements. Developing good SLAs involves "knowing your operation and understanding the ranges proposed by the vendor," according to Petty. "The numbers are sometimes a shot in the dark," he says. "That goes back to pressing the provider on what the numbers are based on and really understanding what they mean."

Most SLAs focus on uptime and availability, but other factors are important, including performance when demand spikes and manageability, according to Sanders.

While SLAs hold providers to their side of the bargain, government leaders also have the responsibility to manage within what Petty calls the "assumption ranges" specified in those agreements, along with understanding what happens when demand goes beyond those parameters. "This is an area where if it is not clear, people will have to build contingencies in," he says. "It goes back to having a solid understanding of what your needs are. If we understand that clearly, it won't be a surprise."

Managing Cloud Migration Costs

Although governments currently have the potential to leverage pandemic relief funds to support technology modernization, budget constraints remain an ongoing challenge.

Top Strategies:

Create a baseline. Start by determining current operating costs for existing systems. "You have to understand where your cost factors are today, especially if you're transitioning out of an on-premises platform," Petty says. "If you don't understand your current costs, it would be hard to make comparisons." Governments also must account for the costs of managing both on-premises and cloud systems until the transition is complete. Understanding these costs could provide opportunities to help offset cloud migration expenses by selling existing licenses and selling or leasing back on-premises hardware.

Make accurate projections. Estimating costs for new cloud implementations involves developing assumptions about how the new applications and services will be used, including the number of seats or users and the ranges of service levels needed to ensure quality service to constituents or internal business units across a wide range of conditions. These projections can be used to refine the SLAs described previously.

"Procurement is not focused on overages," says Sakati. "Governments need to be more intentional on actual vs. anticipated costs."

Develop systems to monitor costs. Tracking cloud usage and expenditures is important because many governments have experienced budget overages in cloud expenditures. Forty percent of CDG survey respondents familiar with cloud-related expenses said their organizations have gone over budget. About one-third of survey respondents

What is preventing your organization from adopting or more widely using the cloud?*

- **52%** **Financial costs**
- 38% Security concerns
- 37% Lack of trained staff
- 22% Cloud governance/constraints between departments
- 21% Data compliance
- 19% Concern of business continuity
- 18% No need to adopt
- 10% Lack of cloud management
- 18% Do not know
- 6% Other

** Respondents were asked to select their top three priorities from a list of 10.*

(30 percent) have developed mechanisms to track and allocate cloud-related expenses across their departments or agencies, while 13 percent are currently developing these systems.

Consider the costs of switching. One benefit of cloud migration is flexibility — most cloud applications and services can be moved from one service provider to another as needs evolve. Governments must understand, however, what costs are involved in leaving a cloud environment and ensure that high data egress costs built into vendor contracts do not create the same kind of vendor lock-in as legacy systems once did. Nearly one in five (19 percent) survey respondents cited these exit strategies as a challenge with vendor relationships. "If you've locked yourself into a situation because you've sunk all these costs in an inflexible direction, you're not doing yourself any favors," says Sanders.

Ensuring Cloud Security

One longstanding misperception — that cloud is inherently less secure than physical on-premises systems — appears to have abated as governments increase their cloud adoption. "People are getting beyond that," Petty says. However, that growing comfort level has brought with it challenges of its own.

Over half of CDG survey respondents either have not taken steps to improve security in the cloud or did not know if their organization has done so.

Despite the importance of security, government responses to security concerns have been limited. Over half of CDG survey respondents either have not taken steps to improve security in the cloud (23 percent) or did not know if their organization has done so (31 percent). Also worrisome: IT leaders were as likely as their non-technology counterparts to say that no steps had been taken to improve security.

Only one-quarter of respondents (24 percent) have created a cloud security framework. Even fewer have assessed cloud security (20 percent), implemented access or vulnerability management tools (20 and 16 percent, respectively), or inventoried cloud services (18 percent.) (See chart, on page 9.) That creates a significant challenge for CISOs. Ninety-five percent of all cloud-based breaches are the result of incorrectly applied policy settings and security controls as opposed to vulnerabilities in cloud infrastructure, according to research by Gartner.[1]

"All of us using the cloud have to be laser-focused on security vulnerabilities and how they're addressed," says Petty.

Top Strategies:

Evaluate security throughout the enterprise. A holistic approach to security involves examining security across all levels of the IT infrastructure. "That means you have to isolate and control from the core all the way up to the edge, which includes the internet," says Celeste O'Dea, Oracle

managing director of government and education strategic programs. That includes the traditional protections for on-premises systems, as well as access controls that are connected to specific data types and sets.

"Every layer needs to be examined," Sanders says.

Determine standards for safeguarding data. Focus on data — and which sets of data fall under different requirements and standards. For governments, data including sensitive constituent information may fall under a wide range of privacy regulations and standards, including those governing healthcare information and electronic payment data.

Not all data requires the same levels of protection. For example, stringent FedRAMP standards are required for certain types of data used for federal purposes, but it and its emerging StateRAMP counterpart may represent overkill for the majority of local government data.

Working groups can help determine what security standards are appropriate for each set of data. "One of the most important things is for the auditor, CISO, attorneys and business owners to have a common understanding," Petty says.

Evaluate vendor capabilities. Cloud service providers typically have resources that few individual organizations can match, including sophisticated applications that leverage artificial intelligence and machine learning (AI/ML) to detect and respond to threats. However, it is important to ensure vendors divulge their own security certifications and procedures for ensuring transparency around security breaches and responding to them. "You can't come in after the fact to make sure they have appropriate security controls," Petty says.

An emerging area of concern involves managing supply chain risk, which in the digital world could mean a vendor obtains software or hardware with vulnerabilities which, in turn, compromises their operations and those of their customers. Ensuring vendors have cyber risk management policies for their own suppliers is becoming increasingly important.

"It is a new area that frankly most states are not looking at — they have their hands full taking care of their own security," Petty says.

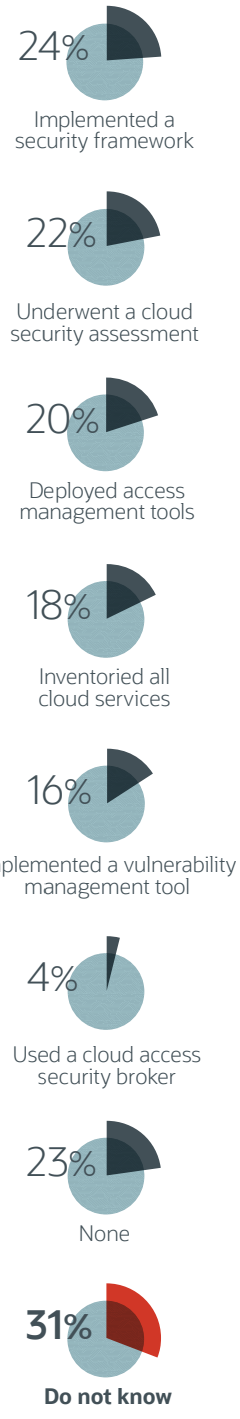
Commit to monitoring security. Including standards in procurement requirements is not enough to ensure government systems are secure, Petty cautions. Because the vast majority of cloud security breaches come from the client side, governments share responsibility for ensuring their employees are following policies and they are securing data in appropriate ways.

"It's the ongoing posture of the organization that matters," Petty says. "Having some kind of monitoring program is really critical."

Developing an Enterprise Strategy

Governments are recognizing the importance of taking an enterprise approach to cloud challenges. Nearly one-quarter of IT leaders responding to the CDG survey (23 percent) say their agencies or departments have developed enterprise cloud strategies — and nearly twice as many (39 percent) are currently developing them. Even so, governments need to take a more systemic approach

What has your organization done to improve security in the cloud?



to cloud implementation, says Sakati. "Enterprise evolution has not caught up to the reality," she says.

Top Strategies:

Include all stakeholders. A majority of survey respondents said department leadership and IT staff join enterprise IT in developing cloud strategies. Bringing business owners and IT leadership together is critical to avoid fragmentation and create a common understanding of business objectives and the scope of cloud projects.

These joint conversations can eliminate confusion about service models. "The CIO may see [a project] as an infrastructure-as-a-service solution and understand there are shared responsibilities between the provider and the state, but someone in the finance or auditor's office may see it as a software-as-a-service solution," says Petty. "If they are seeing it from different perspectives, they are all in for a rough time."

Evaluate input from partners. Traditional technology partners, including consultants and system integrators, are often involved in the development of enterprise strategy. More than 70 percent of CDG survey respondents said these partners are involved in the process. Because system integrators and consultants play such an outsized role in planning, it is important to "make sure they're headed in the same direction you need to move for cloud adoption," Sakati says.

By contrast, fewer than half of respondents included cloud providers in strategy development, which Petty believes is a mistake. "Government should be having discussions during their market analysis and strategy development with industry and providers to understand the full range of up-to-date solutions available to meet their business needs," he says.

Prioritize modernization projects. Cloud platforms provide governments with opportunities to deploy applications quickly in response to changing needs. An enterprise strategy that includes the needs of business units can help IT leaders identify priorities for modernization and, as was the case during the pandemic, be prepared to launch new digital services as needed.

"When we can be that agile in our business solutions, that prepares us to optimize the cloud," Petty says.

Bring an enterprise approach to procurement. An enterprise approach also can simplify the process of procurement. "More and more governments are understanding they cannot do a one-off procurement for every cloud solution or every business solution out there," Petty says. A comprehensive roadmap can allow agencies and procurement officials to create umbrella contracts or prequalify vendors to move quickly as business needs evolve.

☑ LOOKING AHEAD

Effective cloud strategies and policies will be critical as governments move forward, building on the rapid progress made creating digital services and workflows during the pandemic to create more permanent structures.

"The timelines seen in COVID are not going back," says Petty. "When there is a business need, we have to be able to deliver quickly."

For that reason, cloud will play an essential role in modernization plans. The days of "cloud first" and "one cloud" are gone, replaced with an imperative to deliver the optimal solution for governments exploring hybrid or multi-cloud solutions. Only when governments develop systems to plan, procure and manage services will they be as responsive as the technology's potential.

"Think big, start small, scale quickly, fail fast and be adaptable," Sanders advises.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Oracle.

1. HTTPS://WWW.GARTNER.COM/EN/DOCUMENTS/3850266/CLOUDS-ARE-SECURE-ARE-YOU-USING-THEM-SECURELY-0
IMAGES PROVIDED BY SHUTTERSTOCK.COM
CHARTS SOURCE: CENTER FOR DIGITAL GOVERNMENT CLOUD PROCUREMENT SURVEY, APRIL 2021

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: ORACLE

Oracle offers suites of integrated applications plus secure, autonomous infrastructure in the Oracle Cloud. For more information about Oracle (NYSE: ORCL), please visit us at **www.oracle.com.**