UNDERSTANDING CLOUD PROCUREMENT:

A GUIDE FOR GOVERNMENT LEADERS

For years, cloud computing has been top-of-mind for state officials throughout the country – and many leaders have determined it's a viable way to achieve IT modernization. New research from the Center for Digital Government (CDG) finds 55 percent of states have adopted cloud to update their email systems and 42 percent have implemented cloud-based content management systems.

Yet, despite devoting significant time and money to cloud adoption, many government leaders still find themselves searching for the right formula to capitalize on cloud's potential.

A top challenge: procurement. After all, acquiring cloud services is not the same as purchasing a physical commodity. What are the best practices for procuring something as unique as cloud? CDG's research identifies the biggest barriers to cloud procurement and offers guidance to government leaders.

One of the most important study findings? Government officials say they need a guide to help them overcome the challenge of buying something that diverges from more traditional resources.

This paper provides a procurement checklist to give government officials a starting point on their cloud journey. It outlines what's needed for a forward-looking cloud procurement strategy. And while a long-term plan is essential, for the immediate future, the most common IT model in government will be a hybrid infrastructure of on-premises data centers and cloud services. Blending these options is an important consideration.

CLOUD PROCUREMENT ROADBLOCKS

The decision has been made: At least some portion of your IT environment will move to the cloud. Now obtaining cloud services that meet mission goals and deliver on performance requirements is in procurement's hands. Unfortunately, CDG survey results show that most state and local organizations struggle with this essential second step, which can inflate costs and delay transformation at a time when constituents demand faster, better services from their governments. Factors that derail cloud procurement success include:

THE CDG SURVEY FOUND ONLY 42 PERCENT OF SURVEY RESPONDENTS HAVE FORMAL CLOUD PROCUREMENT METHODOLOGIES THAT COVER SUPPLIER EVALUATION THROUGH RELIABLE PERFORMANCE MONITORING.

Lack of a formal cloud procurement roadmap. The CDG study found that less than half of the survey respondents (42%) have formal cloud procurement methodologies that cover supplier evaluation through reliable performance monitoring. Instead of following a cohesive plan that approaches cloud acquisition strategically while preserving existing on-premises IT investments, governments often create ad-hoc processes and rush to adopt cloud to meet the specific needs of an individual department.

This one-off approach extends to vendor selection. Thirty-seven percent of respondents say they evaluate providers on an ad-hoc basis, and less than half (47%) have formal due-diligence policies in place to evaluate cloud providers. This lack of upfront planning can lead to unanticipated consequences. For example, agencies may overlook statewide data security and governance policies, which could expose sensitive government information.

RESEARCH METHODOLOGY

Oracle commissioned CDG to perform national research on state cloud procurement challenges. CDG conducted 16 phone interviews in May and June 2017 with 24 state IT and procurement officials, and gathered an additional 66 responses from state IT and procurement employees involved with cloud procurement through an online survey fielded in June 2017. In total, CDG collected responses from 82 individuals representing 38 states.

The research data and this resulting guide are intended to help governments adopt cloud more effectively and ultimately gain more value from these solutions. "Oracle customers are embracing our cloud solutions as we remain a valued partner in modernizing applications and technology," says Dennis Morgan, group vice president of public sector channels for Oracle. We commissioned this research and created this guide based on our customers' quest for information in their journey to the cloud.

Unfortunately, even those with formal roadmaps often lack confidence in them. Almost 30 percent of respondents with a cloud procurement plan say it was developed internally and may be insufficient.

Not enough information to determine security requirements. Procurement officials responding to the CDG survey say they often lack data classification information when they receive cloud procurement requests. This can make it difficult to determine the appropriate level of security needed for data that will move to the cloud. For instance, some data is highly sensitive and is protected by regulations such as HIPAA, but other information may already be available to the public. Certain security levels can also incur more costs — fees for FedRAMP "high" may be higher than for lower levels. Understanding data security requirements is crucial for finding a cost-effective solution and ensuring the right vendors are involved in the procurement.

Procurement and IT teams do not collaborate effectively. Nearly one-third (32%) of survey respondents say this prevents successful cloud procurement. Close communication between these teams is essential to understand fundamental issues such as data classifications (mentioned previously) and how new cloud services will integrate with an organization's existing systems.

Traditional procurement processes are not structured to acquire services. Since cloud procurement does not fit the traditional purchasing model, contracts are not typically set up for it. While many states (79%) procure cloud services through state contracts, a sizeable proportion (37%) also buy through one-off agreements, which can create frustration due to a lack of standardization. Interviewees want their states to have access to as many cloud options as possible.

To sort out these overarching cloud challenges, some states have developed more formal guidelines. For example, Mississippi created an enterprise cloud policy that considers the state's private cloud as a first option for agencies. If that doesn't meet unique agency needs, it offers guidelines to migrate to the cloud.

The commonwealth of Virginia has also taken steps to formalize a cloud procurement process. The state developed a comprehensive cloud policy that paves the way for agencies to move to the cloud in a responsible and safe manner.

MISSISSIPPI CREATED AN ENTERPRISE CLOUD POLICY THAT CONSIDERS THE STATE'S PRIVATE CLOUD AS A FIRST OPTION FOR AGENCIES. IF THAT DOESN'T MEET UNIQUE AGENCY NEEDS, IT OFFERS GUIDELINES TO MIGRATE TO THE CLOUD.

THE PROCUREMENT CHECKLIST:
BEST PRACTICES TO PURCHASE CLOUD SOLUTIONS

THE FOLLOWING CHECKLIST HIGHLIGHTS THE AREAS GOVERNMENTS SHOULD CONSIDER WHEN PROCURING CLOUD SERVICES.

UNDERSTAND NEW BUDGET AND WORKLOAD REQUIREMENTS.

A shift to the cloud is a departure from traditional purchasing processes. Procurement officials need to think about the changes this will introduce to budget planning and resource allocation.

HOW DOES THE BUDGET NEED TO BE REALLOCATED?

Cloud services are procured via subscriptions, which is a shift from capital to operating expenses. Potential benefits of this model include less upfront investment and more predictable fees.

Officials must understand other nuances when moving away from a fixed payment model. For example, capital spending for new data center equipment may be significant, but multiple budget cycles may pass before IT requests more funds for the same type of hardware. Not so with cloud services. New funds are allocated each year to maintain or, if necessary, increase the existing levels of cloud services.

In addition, officials must look beyond first-year costs by conducting a three- or five-year total cost of ownership (TCO) assessment for standard business applications and infrastructure services to ensure accurate comparisons. For economic analyses of large-scale projects, such as moving to a new enterprise resource planning (ERP)

platform, some cloud experts advise forecasting 10 years out to adequately compare the TCO of on-premises infrastructure to cloud alternatives.

HOW MUCH STAFF TIME NEEDS TO BE DEDICATED, AND WHAT SKILLS ARE REQUIRED?

Staff time must be allocated to monitor vendor performance and manage service contracts. Unlike a one-time buy, these are ongoing functions. Organizations will need to plan for these activities and develop the contract management skills necessary to perform them.

WORK CLOSELY WITH IT.

To ensure successful cloud procurement, IT and procurement officials need to work together regularly before, during and after acquisition.

DO YOU HAVE A WORKING GROUP ESTABLISHED THAT INCLUDES IT AND PROCUREMENT OFFICIALS?

The main responsibility of the working group should be to focus on the technology being acquired. These stakeholders can outline cloud needs for the scope of work within requests for proposals. In addition, they can identify cloud subscriptions that add technology to the IT environment versus services that will replace existing on-premises licenses or hardware. Distinctions like these will be important to estimate capital and operating expenses.

This group should also consider the costs to integrate cloud services within the existing data center environment, the likely expansion of cloud and how contracts will be funded year over year.

DETERMINE SECURITY AND COMPLIANCE REQUIREMENT S FOR DATA.

It's no surprise that security is important to government officials. Seventy-four percent of survey respondents said security regulations and requirements are top influencers when choosing cloud providers, and 55 percent said they evaluate vendor performance in part by compliance with federal regulations, such as FedRamp.

DO YOU KNOW WHAT SECURITY STANDARDS ARE APPROPRIATE FOR THE DATA MOVING TO THE CLOUD?

Certification processes, such as those for FedRAMP, HIPAA and CJIS, may exclude potential cloud providers from consideration when procuring services. Specifying advanced security certifications for routine data can limit competition and increase costs unnecessarily.

HOW IS DATA SECURED WITHIN THE CLOUD DATA CENTER?

Understand the cloud provider's capabilities for access controls that manage who can view and edit data. Also analyze how providers segment data within multi-tenant environments to ensure only the actual owners of the information can view it.

HOW COMPREHENSIVE IS THE SERVICE PROVIDER'S SECURITY STRATEGY?

When procuring cloud services, officials should have a clear understanding of how data will be protected: How are the data center facilities secured? Do the facilities and personnel meet applicable security/privacy requirements? What's the cloud vendor's liability in the event of a data breach? How does it handle necessary security audits, and how will clients be notified of security incidents and/or data breaches?

For help in framing a comprehensive list of questions, refer to cybersecurity publications from the National Institute of Standards and Technology (NIST)[1] and guidelines from the Cloud Security Alliance.[2]

To ensure service providers comply with the security terms specified in contracts, some states hire a third party to conduct SOC-2 audits created for service organizations by the American Institute of CPAs.[3]

SPELL OUT WHO O WNS GOVERNMENT DATA AND HOW IT WILL BE MANAGED.

Sending sensitive data outside the confines of an onsite data center can be risky unless government officials and service providers are in sync regarding data management.

WHO OWNS THE DATA?

Procurement officials may assume ownership doesn't change just because information is stored in someone else's facilities, but assumptions like these can be dangerous. It's important to ensure contracts clearly state the government retains ownership of its data. If certain data will be encrypted in the cloud, officials should insist on controlling the encryption keys to retain access to the information.

IN THE EVENT THE CONTRACT ENDS, IS THERE A WORKABLE PLAN TO RECOVER DATA?

It is also important to understand what happens if the cloud provider becomes insolvent or ceases to operate. Clear terms for data portability ensure states can retrieve their data if they choose to partner with a different cloud provider, or if their current vendor runs into financial or security challenges. Standard APIs facilitate data portability. Some states, such as Virginia, also insist on escrowing content, where copies of data are stored not only in the service provider's primary facilities but also backed up to a public cloud service.

WHERE WILL THE DATA BE STORED AND WILL YOU BE NOTIFIED IF THE DATA MOVES?

Knowing the physical location of data is important for government organizations that are bound by regulations or internal policies for keeping information within U.S. data centers. Executives may also prefer cloud facilities that are accessible for onsite visits by their staffs. These reasons make location a top consideration for state IT and procurement officials. Two-thirds of the survey respondents cited the location of the data center as something they wanted to know before procuring cloud services.

CREATE FORMAL POLICIES FOR VETTING VENDORS.

Not all cloud service providers are equal, which is why procurement officials must evaluate potential vendors using a range of criteria.

WHAT IS THE CLOUD VENDOR'S REPUTATION?

It's important to look at a potential vendor's size, financial strength, and technical and security expertise. Answers to the following questions will help procurement staff investigate the cloud vendor's reputation:

- Who owns the data center and the resources inside it, and who manages the facility?
- What other manufacturers or technology does the data center rely on to perform this service?
- Do potential cloud services use open source technology and open industry standards to ease data integration?
- Is the service provider willing to negotiate certain terms of pre-established service level agreements (SLAs)?

Procurement officials can also use customer references, peer contacts at industry groups such as NASCIO and the rankings of research organizations to assess the industry status of service provider candidates.

DOES THE VENDOR HAVE EXPERIENCE IN THE GOVERNMENT MARKET?

Cloud applications that successfully serve commercial enterprises may not automatically translate to the public sector. For example, government organizations must adhere to some data management and procurement regulations that don't apply to industry.

WILL THE VENDOR SUPPORT A HYBRID CLOUD ENVIRONMENT?

Procurement officials should find out if the cloud provider can provide the same functionality for licensed software running in an on-premises data center or if certain capabilities come only with cloud subscriptions. Vendors who can do both are better positioned to support hybrid cloud environments, which cloud managers in government expect will remain a familiar model in the years ahead.

DOES THE SERVICE PROVIDER OFFER PRE-ESTABLISHED SLAS?

Finally, determine whether the service provider offers pre-established SLAs. Well-defined SLAs are essential to ensure a provider will meet a government's requirements and to enforce contract terms. But there should be room for negotiation. Some cloud vendors try to optimize their costs by delivering the same levels of service to as many clients as possible. If the standard contract isn't right for the state, get a clear summary of any additional charges for a heightened SLA.

CONCLUSION: THE TIME IS NOW TO CREATE A CLOUD PROCUREMENT STRATEGY

Many governments have made the decision to move to cloud, but procurement challenges continue to hinder implementations. This paper offers new research and a checklist of best practices to help states overcome these hurdles and position their organizations to deliver modern government services. It's important to remember that for the immediate future, hybrid combinations of on-premises data centers and cloud services will be the predominant IT model in government, but it's never too early to start a formal cloud procurement strategy.

Endnotes:
1. https://nvd.nist.gov/800-53/Rev4
2. https://cloudsecurityalliance.org/
3. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx

HYBRID COMBINATIONS OF ON-PREMISES DATA CENTERS AND CLOUD SERVICES WILL BE THE PREDOMINANT IT MODEL IN GOVERNMENT, BUT IT'S NEVER TOO EARLY TO START A FORMAL CLOUD STRATEGY.

IMAGES PROVIDED BY SHUTTERSTOCK.COM

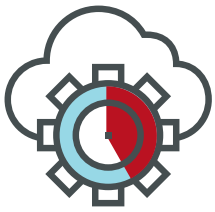
TAKING THE PAIN OUT OF CLOUD PROCUREMENT

Despite focusing significant time and money on cloud adoption, many government leaders still struggle to capitalize on cloud's potential. The Center for Digital Government (CDG) wanted to know why.

With support from Oracle, CDG surveyed and interviewed 82 state IT and procurement officials in June 2017. The paper, "Understanding Cloud Procurement: A Guide for Government Leaders," analyzes the findings and presents a cloud procurement checklist to help leaders better navigate cloud adoption and IT modernization. Here are some key findings:

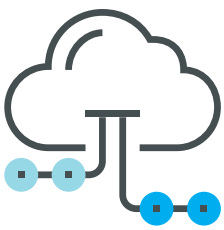
CLOUD OFFERS A VIABLE PATH TO IT MODERNIZATION

42%
of states have
CLOUD-BASED CONTENT MANAGEMENT SYSTEMS.



55%
of states already use
CLOUD-BASED EMAIL SYSTEMS.

BUT PROCUREMENT SLOWS ADOPTION



Only **42%**
have formal
CLOUD PROCUREMENT METHODOLOGIES.

Only **47%**
have formal
DUE-DILIGENCE POLICIES IN PLACE
to evaluate cloud providers.

GOVERNMENT NEEDS A CLOUD PROCUREMENT CHECKLIST

UNDERSTAND NEW BUDGET AND WORKLOAD REQUIREMENTS.

- How does the budget need to be reallocated?
- How much staff time needs to be dedicated, and what skills are required?

WORK CLOSELY WITH IT.

- Do you have a working group established that includes IT and procurement officials?

DETERMINE SECURITY AND COMPLIANCE REQUIREMENTS FOR DATA.

- Do you know what security standards are appropriate for the data moving to the cloud?
- How is data secured within the cloud data center?
- How comprehensive is the service provider's security strategy?

SPELL OUT WHO OWNS GOVERNMENT DATA AND HOW IT WILL BE MANAGED.

- Who owns the data?
- In the event the contract ends, is there a workable plan to recover data?
- Where will the data be stored and will you be notified if the data moves to a different location?

CREATE FORMAL POLICIES FOR VETTING VENDORS.

- What is the cloud vendor's reputation?
- Does the vendor have experience in the government market?
- Will the vendor support a hybrid cloud environment?
- Does the service provider offer pre-established SLAs?

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 PartnerNetwork

Oracle Public Sector Channels is committed to improving the customer cloud experience with tools, data and solutions to streamline your transition to the cloud. Learn more at **oracle.com/publicsector.**