

Capitals in the Clouds

Part VI: Cloud Procurement: From Solicitation to Signing

NASCIO Contacts:

Meredith Ward
Senior Policy Analyst
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States.

For more information visit
www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@NASCIO.org
www.NASCIO.org

Copyright © 2014 NASCIO
All Rights Reserved

For several years now, the National Association of State Chief Information Officers (NASCIO) has discussed the transition in the state information technology environment as state CIOs sought new approaches to traditional delivery models. The recession prompted state leaders to examine new approaches and leverage technology opportunities. The use of cloud services by state government is the most obvious manifestation of this transition. In 2011, NASCIO launched its Capitals in the Clouds series on this topic. Three years later, states continue to investigate and to leverage cloud solutions, software as a service (SaaS) and infrastructure as a service, with services such as email and data storage remaining the most popular. States have significant experience with private clouds hosted by the state IT organization. Several are in the early stages of sourcing commercial cloud services and third-party cloud hosting. Not surprisingly, the cloud vendor community is ready and willing to respond to the opportunities.

However, as is often the case in state government, it's difficult for the policy, financial, legal and procurement disciplines to keep pace with the rapid advances in technology and associated opportunities for states. New technologies such as cloud services bring the promise of cost efficiencies, flexibility and possibly unintended consequences. State leaders are concerned about the risks. State laws, regulations, and policies are widely seen as barriers to cloud service adoption. In particular, there are concerns that laws, regulations, and policies relating to data privacy and access restrict the CIO's ability to deploy solutions. One example is the storage of sensitive data outside the state's boundaries. Several states are starting to use multi-jurisdictional

and federal cloud procurement vehicles ([FedRAMP](#)). States are also becoming more active in developing procurement and contract templates tailored for cloud services.

As one company puts it, “[in 2014] IT and business stakeholders will move beyond curiosity and take a serious look at adopting next-generation technologies, from software-defined networks and storage to public cloud. As part of this move toward adoption, IT organizations are beginning to explore new ways to actively address challenges around ensuring the performance, availability, and security of their applications and infrastructure.”

NASCIO agrees.

As first reported in the NASCIO/TechAmerica/Grant Thornton 2013 State CIO Survey, [The Enterprise Imperative: Leading Through Governance, Portfolio Management, and Collaboration](#), states continue to turn to cloud solutions, with services such as email and storage remaining the most popular. NASCIO asked respondents about the status of cloud services in their state:

Figure 23
What is your state’s status regarding cloud services?

	Percent
The state is already highly invested in cloud services	6%
The state has some applications in the cloud and is considering others	68%
The state is still investigating cloud services	22%
The state has considered cloud services but has rejected it	2%
Other	2%
Don’t know/does not apply	0%

Source: NASCIO/TechAmerica/Grant Thornton 2013 State CIO Survey

The adoption of cloud services within states represents a dramatic shift in the way states procure information technology (IT) products and services and creating a procurement code to accompany this shift won't happen overnight. As the saying goes, Rome wasn't built in a day. Simply put, states need to change the way they buy, consume, conceptualize and view IT procurement.

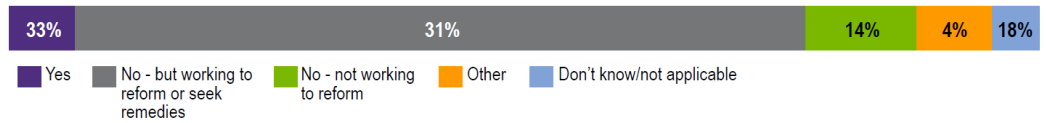
[Creating Effective Cloud Computing Contracts for the Federal Government](#), a joint publication between the Federal CIO Council and the Chief Acquisition Officers Council, sums it up this way: cloud computing presents a paradigm shift that is larger than IT, and while there are technology changes with cloud services, the more substantive issues that need to be addressed lie in the business and contracting models applicable to cloud services.



Indeed it seems that every state is at least thinking about cloud services—and the security, transferability and interoperability of cloud services. Because of this, NASCIO will continue to address these issues in the *Capitals in the Clouds* series. The NASCIO IT Procurement Modernization Committee, in partnership with TechAmerica and the National Association of State Procurement Officials (NASPO), continues to focus on state IT procurement reforms and highlighting best practices at the state level. This brief is a product of the committee and will focus on the range of issues from solicitation to contract signing and future briefs will address implementation and the remaining procurement process.

Getting to the Solicitation Phase

Procuring cloud services compared to traditional IT goods and services can be a different animal entirely, mostly as it relates to the fear of the unknown. That is, state laws, regulations, and policies are widely seen as barriers to cloud service adoption. In particular, there are concerns that laws, regulations, and policies relating to data privacy and access restrict CIOs' ability to deploy solutions. One example is the storage of sensitive data outside the state's boundaries.



Source: NASCIO/TechAmerica/Grant Thornton 2013 State CIO Survey

The above graphic shows that, although a significant percentage of CIOs are unsure whether state laws, regulations, and policies could be a barrier, about half of CIOs believe their current legal and regulatory environment are not consistent with the delivery of cloud solutions. A majority of these CIOs are actively working on changes that will better facilitate and clarify rules governing cloud services adoption.

To aid in addressing such concerns, many states are wisely combatting the unknown with information. For example, the state of **Texas** released [a brief](#) on the benefits of using cloud services and lists these advantages of using cloud services:

- **Reduced Cost** - Agencies can scale back or eliminate expenses and effort related to ongoing IT maintenance, support, and other operations.
- **Instant, On-Demand Services** - Agencies can set up cloud computing services instantly, avoiding long procurement cycles.
- **Pay As You Go** - Agencies pay only for what they use.
- **Rapid Scalability** - Agencies can rapidly increase capacity during peak usage spikes then scale down after peak periods end.
- **Improved Administration** - Agencies can reduce time spent on routine administrative tasks, such as configuration management, manual troubleshooting, software updates, or backups.
- **More Options** - Agencies can customize their solution through an increasing number of service providers, gaining performance and price advantages.
- **Enhanced Reliability** - Agencies can provision disaster recovery and business continuity services.
- **Improved Funding Model** - Agencies can significantly reduce capital expenditures for IT hardware and software and shift to an operating expenditure arrangement.

States Forging Ahead

After a CIO gets over the hump of convincing its state that a cloud model is the best approach in certain cases, what’s next in terms of acquisition? NASCIO also asked state CIOs about how cloud services are procured:

Figure 25

How has your state procured third-party cloud services?

	2012	2013
Used an existing procurement vehicle not specifically designed for cloud services	65%	65%
Created a specific procurement vehicle for cloud services	44%	47%
Leveraged cloud services procurement vehicles created by multijurisdictional consortia	15%	31%
Leveraged cloud services procurement vehicles created by the federal government	6%	16%

Source: NASCIO/TechAmerica/Grant Thornton 2013 State CIO Survey

Several states have already implemented cloud email. In the April 2013 NASCIO/NASTD joint survey on email consolidation, 47% of respondents reported that cloud based email is gaining traction and very comparable with a centrally hosted, on-premise email environment.

States are also implementing other cloud solutions. The state of **Oklahoma** currently has multiple electronic messaging solutions and therefore recently released a solicitation to procure cloud computing as it relates to cloud messaging and cloud collaborative services on a subscription-based model. Some priorities for Oklahoma include providing messaging availability for end-users, reducing statewide information technology (IT) costs and providing a common integrated solution for cloud messaging.

To ensure that the state’s priorities were met, the messaging solicitation included many technical specifications, including retaining ownership of data, on-demand service, maximum availability and end-user performance, rapid elasticity, and tight data security controls.

The Need for Templates

Figure 26

Does your state currently have procurement and contract templates for common cloud services?

	Percent
Yes, specific cloud procurement and contract templates exist and are in use	17%
Yes, specific cloud procurement and contract templates exist but are not yet in use	8%
No, but state is in the process of developing templates	32%
No, but state is interested in developing template	39%
No, not interested	0%
Other	4%

Source: NASCIO/TechAmerica/Grant Thornton 2013 State CIO Survey

States are also becoming more active in developing procurement and contract templates tailored for cloud services, writing standard terms that will protect their state data and citizens. For example, **Colorado** has written a standard model contract for cloud, hosting, and other IT related services. The model contract includes provisions that protect the state’s confidential information:

Use, Security, and Retention

Confidential information of any kind shall not be distributed or sold to any third party or used by Contractor or its agents in any way, except as authorized by this Contract or approved in writing by the State. Contractor shall provide and maintain a secure environment that ensures confidentiality of all State records and other confidential information wherever located. Confidential information shall not be retained in any files or otherwise by Contractor or its agents, except as permitted in this Contract or approved in writing by the State. All confidential information, State data of any kind shall be stored, processed, or transferred only in or to facilities located within the United States.

The Ts and Cs

States are facing common obstacles in the cloud procurement process and are using amended terms and conditions (Ts & Cs) to address these obstacles. For example, **Delaware** adopted a cloud-first initiative in 2011. To ensure that security concerns were addressed by agencies as they acquire cloud services, the Delaware Department of Technology and Information staff invested much time and effort in developing new terms and conditions for inclusion in the state’s standard procurement process.

Delaware has released “[Cloud and Offsite Hosting Specific Terms and Conditions](#),” a 23 point checklist, 9 of which are mandatory and non-negotiable. Like other states, Delaware’s Ts & Cs include provisions mandating:

- Ownership of data;
- Protection of personal privacy and sensitive data;
- Data storage within the United States;
- Proper and timely notification of a security breach;
 - The Service Provider shall inform the State of Delaware of any actual security breach that jeopardizes the State of Delaware data or processes. This notice shall be given to the State of Delaware within 24 hours of its discovery. Full disclosure of the jeopardized data shall be made. In addition, the Service Provider shall inform the State of Delaware of the actions it is taking or will take to reduce the risk of further loss to the State.*
- Public breach notification when citizen personally identifiable information is lost or stolen;
- Legal notices received by the service provider that may require access to data;
- A plan for possible contract termination and return of data to the state including provisions for suspension of services, termination of services, post termination assistance, and secure data disposal;
- Requirements for contractor staff who can access state data;
 - The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State’s information among the Service Provider’s employees and agents.*
- Data modeling and strong password standards.

Delaware also has released a [Cloud and Offsite Hosting Policy](#).

Moving Forward



A recent study from [GigaOM Research](#) reported that, in 2014, the worldwide cloud market is expected to grow by 126%, including a 119% growth in SaaS. It is clear that cloud is here to stay. And [Creating Effective Cloud Computing Contracts for the Federal Government](#) states, “this new paradigm requires agencies to re-think not only the way they acquire IT services in the context

of deployment, but also how the IT services they consume provide mission and support functions on a shared basis.”

And, in NASCIO’s 2013 survey we asked CIOs about their strategies to deliver IT services over the next three years. The four most common responses were:

- Expand an existing managed services model (59%)
- Expand an existing IT shared services model (49%)
- Expand outsourcing (49%)
- Outsource business applications through a SaaS model (49%)

State CIOs understand they must support the business objectives of agencies while also balancing relationships with colleagues such as state budget directors, auditors, technical teams, attorneys general, human resource directors and other agency heads. Certainly creating policies, issuing standard terms and implementing successful cloud procurements will continue in the CIO office and in states as a whole.

NASCIO will continue to address cloud procurement through this series and other avenues.

Reviewers and Contributors

David Ballard
Consultant
CenturyLink Government

David DeBrandt
Worldwide Public Sector
Capture Management
Amazon Web Services

Jane Lacy
World Wide Public Sector
Government and Education Business Development
Amazon Web Services

Rebekah O'Hara
Chief Legal Services Officer, Consolidated Technology Services
State of Washington

Alex Pettit
CIO, State of Oregon

Dugan Petty
Past President, NASCIO

Suzanne Shaw
Of Counsel, Gallitano & O'Connor LLP
Senior Counsel, retired
Washington State Attorney General's Office

NASCIO wishes to thank the states of Colorado, Delaware, Oklahoma & Texas for their contributions to this publication.