OPTUM™

Expanding cloud-based services allows states to be flexible, efficient and save tax dollars

The use of cloud-based services to share resources, software and information is on the rise, and state governments can take further advantage of this technology by learning more about what the cloud offers, how they can store and protect data in the cloud, and how they can revamp procurement processes to realize the cloud's full value.

For states struggling with tight budgets, constant demands and limited IT resources, the cloud and its services can offer much-needed relief. However, understanding what the cloud's features and benefits are, and how cloud providers ensure data security, can seem daunting, especially when states may be considering cloud-based storage for highly sensitive data, such as personal health information.

There is no question that cloud-based solutions, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), are proliferating in the private sector. According to Paul Sallomi, Vice Chairman and U.S. Technology Leader for Deloitte Tax LLP, analysts estimate that the cloud market will "grow from $70 billion to more than $250 billion by 2017,"[1] and predict that "the growth will be driven to a significant extent by enterprises becoming more adept at integrating, aggregating and orchestrating cloud and on-premise assets."[2]

Further, industry analysts predict that "over 90 percent of new spending on Internet and communications technologies … will be on cloud-based technology."[3] And, an IDG Enterprise 2014 "Cloud Computing Survey" found that 69 percent of businesses today are using at least one cloud application, and that investment in cloud technology increased by almost 20 percent between 2012 and 2014.[4]

1. Rebelo, Jagdish, "Enterprise Cloud Computing: Future Market Size, Growth and Competitive Landscape," IHS Quarterly (Q2 2014).
2. Sallomi, Paul, "2015 Technology Industry Outlook," CIO Journal from The Wall Street Journal (Dec. 23, 2014).
3. Hardy, Quentin, "The Era of Cloud Computing," The New York Times (June 11, 2014).
4. "SaaS Gets Its Business Groove On," PYMNTS.com (Feb. 18, 2015).

States also are increasingly adopting cloud services. The 2014 NASCIO State CIO survey found that 73 percent of states have some applications in the cloud and are considering others, while 20 percent are already highly invested in the cloud services.[5]

While state CIOs understand the value of cloud services for states, as NASCIO pointed out, "…it's difficult for the policy, financial, legal and procurement discipline to keep pace with the rapid advances in technology and associated opportunities for states." Laws, regulations and policies are widely understood to be barriers to cloud services.[6] Fully understanding risk is important to creating a balanced approach to advancing state initiatives. A deeper dive into cloud functionality will help policy makers and others better gauge the actual risk and envision a future where server assets can securely and efficiently migrate to the cloud, where elastic capacity reshapes and redefines states' core competencies, and where significant cost savings can be achieved.

Cloud computing, an age old-concept?

Though many of the technologies and the terminologies are new, the core cloud concept of external data and data processing is not. States have been contracting with third parties to perform off site data processing for decades. The following are just a few examples:

Business process	Description	Applications in cloud
Insurance for state employees	States contract payers to manage and process the health insurance for state employees	State employee PHI and PII data are hosted off site. Employees access their profile and claims data via a secure web portal.
Managed Medicaid	States contract payers to manage and process the health insurance for residents	State residents PHI and PII data are hosted off site. Residents access their profile and claims data via a secure web portal.
Health information exchange	Payers publish member data to an information exchange for the state.	Member PHI data is stored in an edge server and accessed by the state over the Internet.

5. NASCIO, "The 2014 State CIO Survey: Charting the Course, Leading Collaboration During Uncertain Times," (September 2014).
6. Meredith Ward, Senior Policy Analyst, NASCIO, "Capitals in the Clouds. Part VI: Cloud Procurement: From Solicitation to Signing," NASCIO Cloud Computer Services, (2014).

States today are successfully implementing a wide variety of external data processing and data hosting solutions in the cloud. While the table summarizes just a few examples, states can also look to other business activities to find that there are many others (e.g. payroll, fulfillment, etc.). When considering the extension of cloud services to health care programs, states could look to these areas to find procurement, contracting and management practices that are already in place that allow third parties to host state data in accordance with state requirements.

What is the cloud and what is SaaS

The cloud and cloud-based services alleviate states' burdens by allowing for fast and easy adoption, ongoing feature upgrades, flexibility to scale up and scale down as needed, and cut application costs. Cloud computing is "a method of configuring and delivering computing power on demand,"[7] according to *The New York Times*. Further, "Individual servers and storage, along with networks and software applications, are pooled and shared by various devices … allowing easier use and higher performance. Usage is frequently metered, like a utility."[8]

Put another way, the cloud offers computing and storage and other capabilities that can be used to build a solution in whole or in part to supplement existing state systems. The term SaaS, which often is used interchangeably with the cloud, is actually a piece of software or a set of software solutions delivered over the Internet. In other words, SaaS is part of the functionality, while the cloud is where the solution resides.

Because the service provider owns and handles the software and hardware necessary to provide the service, SaaS provides states with economies of scale and efficiencies that they cannot get using dedicated solutions.[9]

In the Medicaid arena, when states acquire Medicaid Management Information System (MMIS) solutions, they often acquire highly customized services developed by a systems integrator and place the data in a dedicated environment within the state. When taking the cloud route, a state works with a cloud service provider to migrate the state to an existing Medicaid platform, allowing the state to improve implementation time and achieve economies of scale that they would not achieve on their own.

Indeed, using an existing platform also means the state is not burdened with the development costs or risks, nor must it invest in or be burdened by constantly changing hardware and software technologies. In Kentucky, CIO James Fowler has identified Medicaid as one of the areas of opportunity for cloud application business development. He has stated that "X-as-a-Service" (XaaS) will be explored by Kentucky for storage, telephony and network management, and predicts that his state will be out of the infrastructure market in seven to 10 years.[10]

7. Hardy, Quentin, "Cloud Technology, in Translation," The New York Times (June 11, 2014).
8. Ibid.
9. Center for Digital Government, "Best Practice Guide for Cloud and As-a-Service Procurements" (Sept. 10, 2014).
10. Center for Digital Government, Executive Teleconference with Jim Fowler, Chief Information Officer, Commonwealth of Kentucky, (September 24, 2014).

What are the advantages of the cloud?

States should consider leveraging cloud-based solutions for five key reasons:

1. **Adoption is fast and easy.** Time devoted to installing, migrating, testing and deploying solutions can be done by the cloud providers, leading to a more streamlined transition. SaaS solutions get applications to the market faster, but more importantly, they create value faster.
2. **Features are updated continuously.** The traditional model for business applications requires upgrades and, often, additional investment in underlying technology and other IT resources to take advantage of new features. When states subscribe to SaaS, the upgrade path is streamlined, as the latest features to improve functionality and security are seamlessly upgraded for all clients as soon as they are upgraded for one client. This allows states to react more nimbly and make more informed decisions.
3. **Flexibility is intrinsic to the cloud environment.** One of the distinct advantages of the cloud over traditional outsourcing is the ability to expand and contract on demand, so states can implement change when needed. States may require new features for applications, new functionality, new users or different applications altogether, which can be handled by the provider and, accordingly, conserve a state's IT resources.
4. **Costs are lower.** Because using cloud services lowers infrastructure and maintenance investments, states save money on IT and spend less on manpower. Subscription pricing models allow for more flexibility in licensing than traditional models, including "pay as you go" type models.
5. **IT burdens can be shifted.** States' IT leadership can focus on monitoring versus handling compliance issues, the management of IT infrastructures, the explosive growth in data, and the management of moving-target endpoints.

"Saving money is the number-one benefit cited by businesses transitioning to cloud-based services," according to PYMNTS.com, a business-to-business platform for the payment industry, because "the expense of renting data center space, networking, electricity, cooling and other costs are all shifted to the service provider."[11]

But the value of cloud-based services goes beyond a strict dollar value to include additional benefits. For example, states can more effectively apply the talents of their limited staff to focus on program management instead of duplicating capabilities more effectively delivered by IT vendor partners. Additionally, states could be more responsive to changes in policy and program shifts because of the flexibility of pricing models and the short implementation timeframes for cloud-based services. Today, states can be nimble and flexible, at a reasonable cost — the technology exists today.

11. "SaaS Gets Its Business Groove On," PYMNTS.com (Feb. 18, 2015).

How secure are data in the cloud?

CIOs should be aware that storing data in a private cloud does not necessarily pose a bigger risk than internally stored data. Indeed, because the cloud provider's business depends on the data remaining secure, the cloud provider has great incentive (and the means) to take every possible measure — monitoring, testing, auditing and refactoring — to manage the security of data across the system.

"Cloud software companies, knowing the implications of a crash on their business' bottom line, invest significant resources into insuring that such a disaster never occurs," an article in *Forbes* states.[12] "Cloud computing companies can invest far more resources in data backup and security than your business can."[13]

Indeed, cloud providers have to prove on a routine basis that they can protect a state's data and that those protections can withstand audits as well as federal government scrutiny. Further, there is no guarantee that an internal IT department is managing data any better or worse than a SaaS provider. A state must rely on internal management metrics to ensure the proper the management and protection of application data. Cloud service providers such as Optum address these controls up front during the contracting process and audit them regularly. For example, Optum worked with the state officials of one client to address questions and explain how the private cloud works. The machines, the domains, and the access controls are dedicated solely to Optum. Optum has a corresponding set of controls designed to provide a level of assurance and confidence regarding data access and security.

In this example, hosting and security services start with Optum™ ID service for the application workflow. Applicants must answer various questions designed to prove identity for authorized use and are subject to a series of security controls that align and comply with federal and state-based security frameworks. Optum then continually tests the application code that is submitted, scans cloud boundaries and provides reports back to the states — an active monitoring system designed to reveal any potential security risks and close any gaps that may exist.

12. Savitz, Eric, "Is Your Data Safe in the Cloud?" Forbes (March 6, 2011).
13. Ibid.

The data are thoroughly protected with security codes and role-based security whereby authorized individuals are granted access only to the data they need. Also, the system keeps records of when those people log in to access the data and what they do when they are logged in, all which can be reported back to the state to demonstrate that the security is being maintained.

Optum also has demonstrated its ability to understand security frameworks, as well as to develop an operational plan for how to act in the event of a security incident. Further, states should also be aware that federal agencies, such as the Centers for Medicare & Medicaid Services and the Internal Revenue Service, hold data service providers to regulatory standards that they must meet in order to interface with them.

According to the Center for Digital Government, the ownership, location, and import/export of data are among state CIOs concerns about cloud computing.[14] For example, because public jurisdictions must protect the privacy of certain types of information, including personal health information, protection of data in XaaS is often a shared responsibility, where specific roles and responsibilities should be spelled out in the service-level agreement.[15] These issues should be addressed explicitly in the procurement process, which needs to be revised to accommodate cloud providers and services.

How can the procurement process accommodate cloud services?

When states draft requests for proposals (RFPs), their current boilerplate documents might specify that states build their own computing infrastructure, which excludes cloud and XaaS services. But, when purchasing XaaS, states are buying more than one product or service in a package, and "most states don't have contract vehicles for all those components," Delaware CIO Jim Sills told *Government Technology.*[16] "It is still a challenge to procure," Sills noted, adding that in 2010 Delaware started documenting SaaS terms and conditions instead of reinventing the wheel with each vendor.[17]

Although the private sector has quickly jumped into the cloud marketplace, "government agencies have struggled to embrace hosted services because the cloud often clashes with traditional public purchasing rules and practices."[18] Recently, several states and local governments joined forces with technology providers to tackle updating the procurement process to accommodate cloud technology, and thereby make it feasible for state governments to take advantage of cloud-based services.[19]

14. Center for Digital Government, "Best Practice Guide for Cloud and As-a-Service Procurements" (Sept. 10, 2014).
15. Ibid.
16. Raths, David, "How the Cloud is Changing Everything for Government IT," Government Technology (Aug. 6, 2014).
17. Ibid.
18. Heaton, Brian, "Breaking Government's Cloud Procurement Gridlock," Government Technology (Sept. 10, 2014).
19. "Best Practice Guide for Cloud and As-a-Service Procurements," Center for Digital Government (Sept. 10, 2014).

The resulting "Best Practice Guide for Cloud and As-a-Service Procurements," issued Sept. 10, 2014, states that "if state and local governments want to enjoy the benefits of XaaS, policy makers, finance directors, auditors, procurement officers, attorneys and, ultimately, elected officials, must reconsider and modernize the controls and processes that currently create barriers to accessing these services."

The Center for Digital Government concludes that "procurement processes that require strict conformance to prescribed specifications and unique terms and conditions are ineffective in the current technological environment," and asserts that "It is time to set aside outdated practices that inhibit progress, and move confidently toward a new set of commercially proven practices and procedures that support innovation."[20]

To take full advantage of the benefits of cloud-based technology, states should use the RFP process to:

- define business objectives and measures and not the system requirements.
- link contracts to service-level agreements tied to business objectives and business processes, instead of technology specifications. For example, the RFP should not include language that requires that data must reside "in the state" as part of data security. Instead, it could include a business objective such as "contractor must run auditable daily back-ups to an off-site service provider." In this way, the goal of the RFP language is to ensure data security, not storing data within state borders, which, in and of itself, does not ensure better security.

By shifting the perspective in the procurement process to determine a contractor's demonstrated capability to reduce risk, states will open the door to innovation.

In addition to moving away from requirements-based procurement, the Center for Digital Government offers suggested state procurement approaches that accommodate the cloud and XaaS, such as:

- Take advantage of negotiations
- Keep negotiations moving forward
- Create a negotiations timeline
- Start with a business problem-based solicitation
- Minimize mandatory requirements
- Establish model terms as standards
- Develop national minimum standards
- Improve communication
- Conduct market research
- Use demonstrations
- Implement a multiple round selection process
- Permit multiple awards
- Create alternative sourcing processes

Contact us today to find out more.

Call us at 1-800-765-6092 or email innovate@optum.com.

20. Ibid.

optum.com

11000 Optum Circle, Eden Prairie, MN 55344