NASCIO
Representing Chief Information Officers of the States

NASCIO *Cloud Computing* Series

Capitals in the Clouds

The Case for Cloud Computing in State Government Part I: *Definitions and Principles*

NASCIO Staff Contact:
Eric Sweden
Senior Enterprise Architect
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@AMRms.com
www.NASCIO.org

State government is actively pursuing cloud computing as an innovation it can exploit in balancing two distinct and growing pressures. What is pushing government more and more toward seriously evaluating cloud computing is the present economy. Per the May 2011 National Association of State Budget Officers (NASBO) fiscal survey of the states, state general fund spending is still below pre-recession levels (*see appendix*). Faced with these continued budget challenges state governments will need to find ways to deliver its services to citizens as economically as possible without compromising the achievement of desired outcomes. This new fiscal pressure is actually working to help break down historical barriers to inter-agency collaboration and partnering, sharing services, and pooling of resources.

The other pressure is the drive for innovation as the citizens are facing more uncertainty and complexity in the national and global economy. Innovation demands the ability to continually explore, experiment, and create capabilities quickly. Traditional processes for planning, developing, and testing IT capabilities contrasts with the new need to act quickly when experimenting with new ideas. Cloud computing is an approach that can provide capabilities quickly.

Cloud computing has arrived as a serious alternative for state government. There are outstanding issues that must be faced and dealt with in order to maintain the reliability, responsibility, security, privacy, and citizen-confidence in government services. Government is desperately looking for technology and business process innovations that will make the way for government to deliver existing services more economically. There is also the potential for new kinds of services that may be temporary in nature. Cloud computing provides a number capabilities that have the potential for such innovation.[1]

State government will need to be convinced that future cloud computing offerings can meet its requirements for governance, security, privacy, availability,

elastic demand planning, economies of scale, unambiguous jurisdictional authority, ownership, national security, avoidance of cloud supplier "lock-in", assurance, and citizen confidence.

State CIOs will need to:

- Evaluate cloud computing as an alternative approach for delivering IT services.
- Establish the entrance criteria for considering cloud computing as an option for delivering IT services.
- Examine the impact of cloud computing on federal programs that are administered by the states. Understand the program, legal and policy issues related to the inherent characteristics of cloud computing such as multi-tenancy, and sharing services across government lines of business.
- Develop a cloud computing strategy and evaluation process that involves enterprise architecture, security, records management, procurement, legal, and other expertise centers as appropriate.
- Manage cloud services within the portfolio of government IT services.
- Ensure that business processes are working efficiently and effectively before applying technology to support them.

What is Cloud Computing?

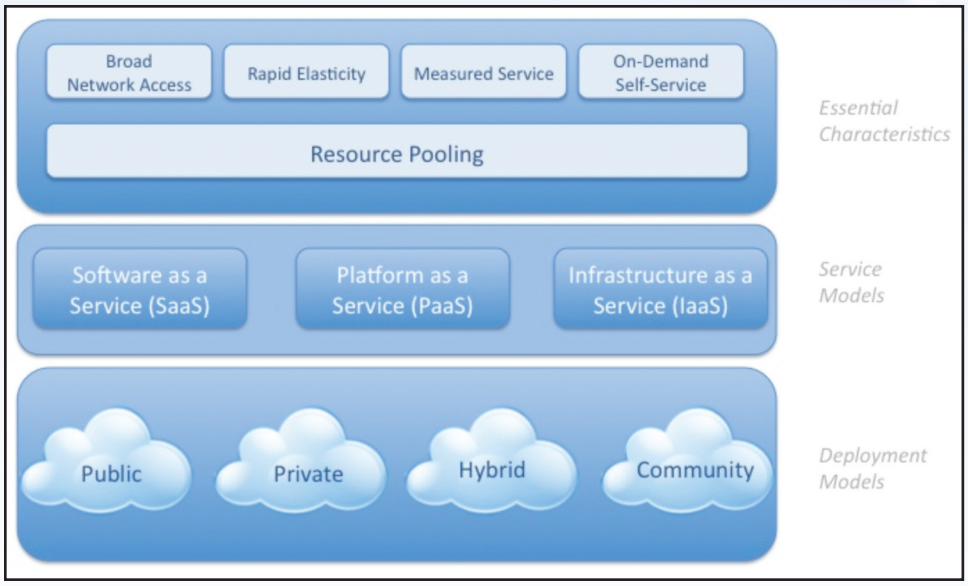
The definitions for the various aspects of cloud computing have been well described by the National Institute of Science and Technology (NIST). NIST has defined the characteristics, the service models and deployment models for cloud computing. Those definitions will be used as foundational concepts for NASCIO's publications on cloud computing. This document summarizes those definitions. This document also presents principles and some of the considerations related to cloud computing for state government to employ in evaluating the appropriateness of cloud computing for a given government asset, function, process, or initiative.

The federal government is actively embracing cloud computing. The Federal Cloud Computing Strategy was released on February 8, 2011.[2] This resource provides invaluable assistance in guiding a cloud computing initiative including:

- The value proposition of cloud computing
- The "shift" in information technology (IT) strategy that is enabled by cloud computing
- A decision framework for migrating to cloud computing
- How to provision cloud services
- Managing services rather than IT physical assets
- Case examples that illustrate the decision framework

Common definitions must be agreed upon so the community of state government is using the same terms in conversation, planning, and execution.

The definitions used herein are those published by the National Institute of Science and Technology.



Visual Model of the NIST Working Definition of Cloud Computing[3]

NIST defined five characteristics the describe cloud computing.[4]

On-demand self-service A consumer can unilaterally provision computing capabilities such as server time and network storage as needed automatically, *without requiring human interaction* with a service provider.

Broad network access Capabilities are *available over the network* and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services.

Resource pooling The provider's computing resources are *pooled* to *serve multiple consumers* using a *multi-tenant model*, with different physical and virtual resources dynamically *assigned and reassigned* according to consumer demand. There is a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources, but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Even private clouds tend to pool resources between different parts of the same organization.

Rapid elasticity Capabilities can be *rapidly and elastically provisioned* — in some cases automatically — to quickly scale out; and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service Cloud systems *automatically control and optimize resource usage* by leveraging a *metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, or active user accounts). Resource usage can be monitored, controlled, and reported.

Cloud Service Models

NIST defines the cloud services models as follows.

Cloud Software as a Service (SaaS) The cloud provider delivers and hosts application(s). The consumer no longer houses or maintains the application(s) in its own data center.[5] The capability provided to the "consumer" is to *use the provider's applications running on a cloud infrastructure*. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

CONSIDERATIONS[6]

- *Who owns the applications?*
- *Where do the applications reside?*
- *Who owns the data?*
- *Where does the data reside?*
- *What are the risks for data corruption in a multi-tenet environment?*
- *Does the contract and/or service level agreement explicitly establish ownership of assets and intellectual property?*
- *What are the non-contractual provisions for assurance?*

Cloud Platform as a Service (PaaS) The cloud provider delivers a development environment where the consumer can create its own applications within the providers computing environment, eliminating the need for the consumer to maintain its own infrastructure.[7] The capability provided to the consumer is to *deploy onto the cloud infrastructure consumer-created or acquired applications* created using *programming languages and tools supported by the provider*. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

CONSIDERATIONS[8]

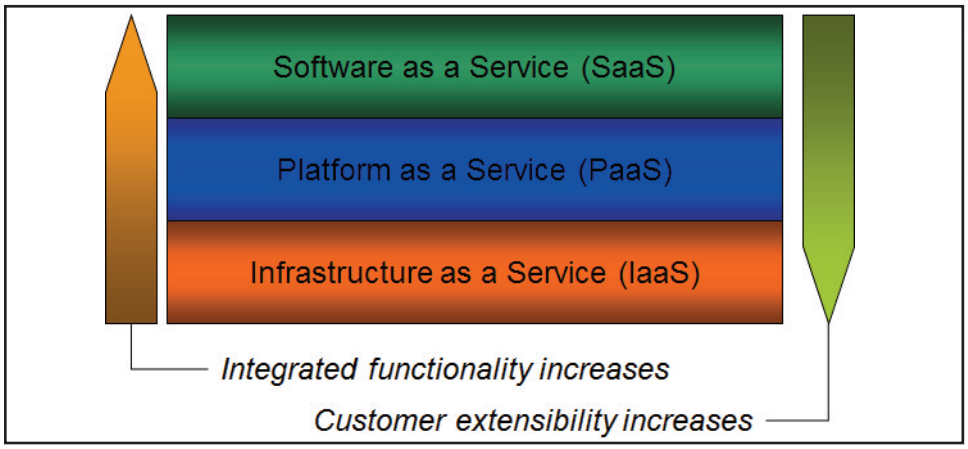
- *What is the availability of the service?*
- *What capabilities exist for ensuring confidentiality?*
- *What provisions exist contractually and programmatically to protect privacy and avoid legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite)?*
- *What provisions exist contractually and programmatically regarding e-discovery?*
- *Same considerations as listed under SaaS.*

Cloud Infrastructure as a Service (IaaS) This allows for the consumer to essentially "rent" a data center.[9] The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where *the consumer is able to deploy and run arbitrary software, which can include operating systems and applications*. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

CONSIDERATIONS[10]

- *What options exist to minimize the impact if the cloud provider has a service interruption?*
- *What is the process for releasing resources once an initiative is completed?*
- *How dynamic is the creation and subsequent release of cloud infrastructure?*
- *What choices does the consumer have relative to technology architecture?*

It must be determined which *service model*(s) are appropriate for the government asset, process, function, or management initiative. The top of the service model stack provides the greatest level of service provider provisioning of security and customer readiness. The bottom of the service model stack requires the greatest level of customer provisioning of security and development of functionality. The IaaS layer provides the foundation for all cloud services. Higher level layers inherit the strengths and weaknesses of the underlying layer in terms of risk, vulnerability and security. There is a balance between functionality and extensibility as indicated.



Cloud Service Models

Cloud Deployment Models

Independent of the particular cloud services model used, NIST defined four deployment models.

Private cloud The cloud infrastructure is *operated solely for an organization*. It may be managed by the organization or a third party and may exist *on premise (internal) or off premise (external)*.

CONSIDERATIONS[11]

- *This is the cloud services option with minimum risk. Anticipate that it may be more expensive.*
- *This option may not provide the scalability and agility provided by a public cloud but may provide greater assurance and security.*

Community cloud The cloud infrastructure is *shared by several organizations* and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

CONSIDERATIONS[12]

- *Same as private cloud, plus:*
- *Data may be stored with the data of other members of the community. This may be appropriate for a given government line of business.*

Public cloud The cloud infrastructure is *made available to the general public* or a large industry group and is owned by an organization selling cloud services.

CONSIDERATIONS[13]

- *Same as community cloud, plus:*
- *Data may be stored in unknown locations and may not be easily retrievable.*
- *Data may be stored in a multi-tenet environment that includes any number of organizations – potentially criminal organizations, or organizations that are under investigation.*
- *Provider may not take responsibility for security, privacy, statutory compliance, etc. Be clear in the contractual terms and conditions as to responsibilities, performance, mitigation, restitution, etc.*

Hybrid cloud The cloud infrastructure is a *composition of two or more clouds* (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

CONSIDERATIONS[14]

- *There may be aggregate risk of merging different deployment models.*
- *Classification and labeling of data will be beneficial to the security manager to ensure that data are assigned to the correct cloud type.*

The Cloud Security Alliance goes a step further to emphasize *multi-tenancy* as a necessary *characteristic* of cloud computing. Multi-tenancy must be understood in order to judge the appropriateness of cloud computing deployment models for a state government services.

The characteristic of multi-tenancy carries with it the necessity to establish unambiguous policies for meeting state government requirements including security, service level agreements, backup and recovery, jurisdiction, and charge-back.[15] Multi-tenancy allows for economies of scale that are achieved through shared infrastructure, metadata, services and applications.

Understand the limitations for each deployment model. Employ the appropriate deployment model based on data and process valuation, reliance, and criticality.

An issue that arises with multi-tenancy is the disparity or diversity of customer requirements. There is an assumption that the tenants of the cloud share similar requirements, or that the cloud provider can gain economics of scale while still meeting a diversity of customer requirements for security, privacy, records management, backup and recovery.

Principles

A grass roots effort called the Cloud Computing Community and Cloud Standards Wikis created a "manifesto" for cloud computing intended to represent the best interests of the consumers of cloud computing services. The Cloud Computing Manifesto (CCMF) presents principles and guidelines that help support and augment the Cloud Computing Bill of Rights. *These principles are intended to be adopted by cloud service providers.*

Principles published as of 2009:

1. Cloud providers must work together to ensure that the challenges to cloud adoption (security, integration, portability, interoperability, governance/management, metering/monitoring) are addressed through open collaboration and the appropriate use of standards.

2. Cloud providers must not use their market position to lock customers into their particular platforms and limit their choice of providers.

3. Cloud providers must use and adopt existing standards wherever appropriate. The IT industry has invested heavily in existing standards and standards organizations; there is no need to duplicate or reinvent them.

4. When new standards (or adjustments to existing standards) are needed, we must be judicious and pragmatic to avoid creating too many standards. We must ensure that standards promote innovation and do not inhibit it.

5. Any community effort around the open cloud should be driven by customer needs, not merely the technical needs of cloud providers, and should be tested or verified against real customer requirements.

6. Cloud computing standards organizations, advocacy groups, and communities should work together and stay coordinated, making sure that efforts do not conflict or overlap.

Additional Principles to be Considered

The cloud computing business model is generally contrary to tailored, or customized services and contracts. Uniqueness in delivery is in opposition to the gains in economies of scale that create the viability of cloud computing.[16]

1. Cloud computing solutions must offer and provide the same or better security capabilities as traditional in-house infrastructure, network and applications.

2. State government must not find itself in a "lock-in" position where its power of negotiation is compromised. This becomes an issue when state government moves beyond the private cloud into the other deployment models. The risk and/or reality of lock-in increases moving up the architectural stack. The greatest risk for lock-in is at the application layer.[17]

3. Cloud computing must not create a vulnerability for loss of confidential information or for maintaining national security.

4. Cloud computing must not put the information of citizens at risk for data breaches, identity theft, or unwanted marketing.

5. Cost is a major motivation for migrating to cloud computing. That motivation must persist going forward. That is, it must always be significantly more economical to pursue a cloud computing strategy than traditional approaches for infrastructure, platform and software services.

6. The customer must beware – as the customer commits to a more external cloud, risk increases. As the customer moves up the architecture layers from infrastructure to platform to application, risk increases. This increase in risk is partially due to the fact that each architecture layer inherits the risk of the underlying layer.

7. Cloud computing alternatives must be evaluated using a total cost of ownership, and long term cost of ownership.

8. Migrating to a cloud computing strategy must by necessity involve a loss of operational control over quality of service, variability in the location of data, potential for data breaches, potential for cloud provider lock-in, issues of information stewardship, and dependence on cloud provider for continuity of operations. These losses are mitigated through moving toward a more conservative strategy. Risk is reduced as the customer moves from public to community to private cloud strategies.[18]

9. Cloud strategies must include evaluation of physical security, internal controls and oversight, emergency response procedures, authorization, authentication, identity management, and privacy. Essentially, the same discipline for evaluating security for conventional computing architectures.[19]

10. In a cloud computing architecture, uniqueness drives up cost and thus compromises the economies of scale that justify a cloud computing strategy. Standardization and common approaches drive down cost and thus help achieve the economies of scale that justify a cloud computing strategy.

11. Economies of scale are easier to achieve moving down the architecture stack. The most achievable economies of scale are in the infrastructure layer.

12. Migrating to a cloud strategy must entail a carefully planned and executed strategy for organizational change.[20]

13. Government records managed in a cloud environment are subject to the same laws and regulations as government records managed on agency owned systems. The location of the data does not compromise or modify the original records management and preservation requirements. A cloud computing alternative must provide the same or better compliance with government requirements as government owned systems.[21]

14. Government must anticipate cyber pirating and take the necessary administrative, legal, physical, and technological measures to ensure such pirating is prevented, detected, and mitigated. Government cannot rely on service level agreements, or contracts to allay the risk of pirating. Anti-pirating strategy must be deliberate, taking into account the fact that US law is not enforceable internationally.

15. With potential increased ease of use, flexibility and means for managing elasticity, usage rates of some applications may increase. That will impact the cost/benefit analysis that originally justified the cloud computing migration project. Such behavior essentially uncovers pent up demand for services that didn't surface under early computing models. Nevertheless, such outcomes may arrive to eliminate some portion of the cost savings anticipated. Anticipate that the demand equation changes.

First Things First

Governance **-** As with any new arrival on the technology scene, there is the early introduction followed by the proliferation stage and accelerated adoption, then a maturing, and the rationalization of the technology which leads to establishing good management practices and governance. Governance is essential to avoid uncontrolled proliferation of technologies and subsequent commitments. Governance provides a disciplined, rational evaluation of alternative capabilities for delivering on the strategic intent of the organization. Governance can be simply defined as establishment of decision rights and oversight to ensure the initiatives deliver the benefits sought, the initiative is aligned with the strategic intent of the government agency, and proper employment of necessary capabilities to enable the initiative. Proper governance encompasses all of government and brings IT and the business together as partners. As described in NASCIO's publication, *IT Governance and Business Outcomes – A Shared Responsibility between IT and Business Leadership*, governance is all about ensuring that state government is effectively using information technol-

ogy in all lines of business and is leveraging capabilities across state government appropriately to not only avoid unnecessary or redundant investments, but to enhance appropriate cross boundary interoperability.[22]

Governance of cloud computing must include technology, organization and culture, supplier management, and portfolio management. Relative to cloud computing, proper governance will ensure that cloud services are orchestrated, rationalized and optimized from an enterprise perspective. This will help ensure contracting of services is proactively managed and uncoordinated contracting of cloud services does not occur. Without proper governance agencies can easily engage cloud services independently which can result in redundant investment; inadequate or absent vetting of providers; inattention to statutory obligations; increased security and legal risk for the state. Proper governance should be created with the following components:

Organization - A new organization is not being prescribed. Rather, the existing governance for state government IT should encompass evaluation and appropriate employment of the various cloud strategies within the overall enterprise governance established in the office of the state chief information officer. This includes the proper alignment of cloud services with initiatives where indicated; proper employment of appropriate service models and deployment models; ongoing monitoring and evaluation of cloud services. Further, cloud computing should be an integral component of the state government enterprise architecture. Cloud computing essentially constitutes an approach for engaging IT services. Therefore, service management approaches will be relevant to cloud service management. There is the added dimension of managing relationships with external providers in a way that may be significantly different from previous vendor management. In the case of cloud computing, the provider may have applications, data, and intellectual property in residence. Therefore, there is the need for greater trust and assurance. The governance organization may actually include representation from these trusted partners as decision makers and advisors.

The Cloud Strategy – Like any product or service, cloud services must be managed through the use of a strategy for proactively harvesting the value of cloud computing. A strategy for cloud computing should begin with the strategic intent of state government, and/or the state government agency. As described in the NASCIO Enterprise Architecture Value Chain, strategic intent is enabled through capabilities.[23] Cloud computing is essentially a capability, or set of capabilities that are available for enabling strategic intent. Cloud computing should then be seen as a technology choice that will be evaluated for appropriate service types. For example, services that can be described as non-mission critical, or commodity services, make the best early targets for cloud computing. The cloud strategy will describe what service types will be delegated to cloud computing. Selection criteria should be developed for evaluating government IT services in order to identify appropriate IT service candidates. This will include a risk assessment of the government IT service, including the criticality of the IT service. Components of state government IT governance should include the following components related to cloud computing:[24]

- *Cloud lifecycle management*
- *Cloud planning, modeling, architecture, deployment*
- *Cloud onboarding and offboarding*

- *Cloud portability*
- *Cloud requirements analysis*
- *Cloud operations and sustainment*

The Cloud Portfolio – cloud services should be proactively managed within a cloud portfolio using the similar techniques employed in financial investment portfolio management. That "services" portfolio will change over time. Some cloud services will be traded out for other cloud services. Some cloud services may be added for a short period of time and then eliminated once they are no longer needed. Other such services will be enhanced with additional features. Cloud portfolio management will include the onboarding and off-boarding of cloud services, selection of deployment models, selection of services models, evaluation and selection of service providers, and portfolio risk management. Portfolio management must include the rationale and criteria for prioritizing the demand for cloud computing.

The cloud portfolio is part of the services portfolio. The services portfolio is a component of the enterprise IT investment portfolio. Keep in mind, not every service will be deployed as a cloud service. Not every IT investment will necessarily be a service.

Cloud Analytics – Cloud analytics will be used to monitor and evaluate performance and availability of cloud services in comparison with state government cloud policy and strategy. Cloud analytics will assist in optimizing capacity planning and minimizing the premium paid for unused resources. The performance target is to pay only for the capacity used. This will require growing the capability for forecasting demand. Going forward, this may become the one of the most important competitive metrics for cloud providers and customers.

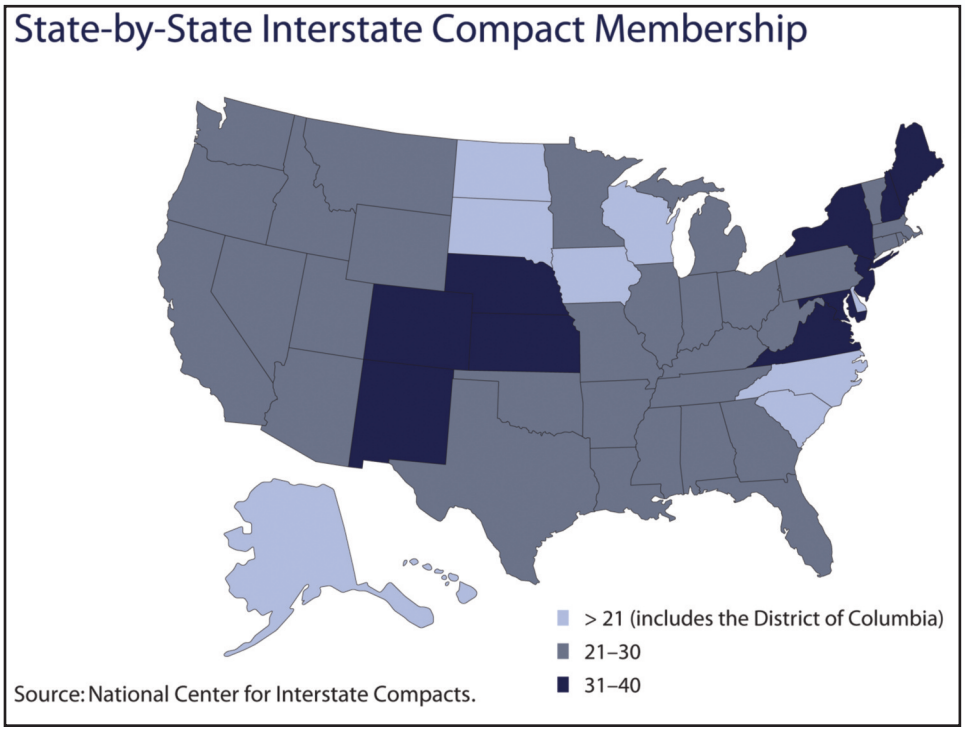
Analytics will continually be evaluated to either justify or challenge sustaining a cloud service. The economic premise for cloud computing is an emphasis on variable costs versus fixed costs. Cloud computing has arrived on the scene as a defensible alternative to making capital investments in hardware and software because the variable costs associated with "renting" these resources is so inexpensive. This approach is also justified now because services can be discovered, evaluated, and engaged so efficiently in today's internet enabled economy. However, recall that in the first half of the 20th century, services were brought into the enterprise because of the high cost of searching, contracting, coordinating and paying for external services.[25] The proverbial pendulum can swing back again in the future. If that swing occurs, it will be initiated by analytics and performance metrics that justify bringing services back into the enterprise. Therefore, state government must think about an exit plan with any external service provider.

Financial Considerations - Funding models are necessary to support enterprise cloud deployment. These models should include the financial mechanisms employed that will facilitate appropriate sharing of the costs as well as the savings, maintenance and sustainment of program and project management, legal fees, indemnification, training, and other considerations.

As state government moves into a cloud services deployment model, there is a migration away from capital investment budgets and systems acquisition to acquisition of services that may entail no capital investment. That is a significant change to past operations and will require states to reexamine their capital budgeting process, funding models, and incentives. For some cloud deployment models, the historical pattern of systems acquisition, system operations and maintenance, and systems refresh cycles are replaced with new IT management disciplines for managing services. Movement away from the traditional model for delivering IT services will have a significant impact on staffing, training and employee development, skills inventories, and career paths. These issues become most relevant for public, hybrid, and community cloud deployment models.

Multi-State Collaboratives – This aspect of governance constitutes the customer side of the transaction. It answers the question regarding WHO will participate in negotiating and employing cloud services as a community of consumers. State governments are very comparable in terms of functions which leads to the conclusion that states are very comparable in terms of government services and government IT services. If that is true, then the question arises, can states develop solutions together that achieve economies of scale on the consumer side. The result would be a portfolio of approaches depending on the characteristics of the government IT service and would include private, community, and public cloud solutions. Further, such a portfolio of cloud services could include services that are shared by all levels of government.

The advent of multi-state compacts occurred as early as 1783. Between 1783 and 1920 there were 36 interstate compacts created. Most of these were created to settle boundary disputes. Today there are more than 200 interstate compacts. Twenty-two of these compacts are national in scope.[26]



An example of a loosely formed compact is the western states GIS collaborative. Colorado, Montana, Oregon and Utah issued a request for proposals for a commercial cloud storage provider to host the states' GIS data instead of each state negotiating its own separate contract. The western states initially sent out a request for information (RFI) in November of 2010. Many compacts will have a named "lead state" that will formally negotiate for the compact states. The GIS RFI collaborative is led by the state of Montana. All of the members of the GIS collaborative are also members of the Western States Contracting Alliance (www.aboutwsca.org). WSCA supported the collaborative by formally issuing the RFI. The member states formed an assessment team that reviewed the 23 responses to that RFI and reported the results.[27] The next step for this initiative will be a request for proposal (RFP).

This collaborative could easily set the stage for other similar collaboratives, or formal compacts. Formation of national alliances, collaboratives, and formal compacts can be expected to proliferate in the future. Memberships will assuredly include local and federal government as well.

The sharing of IT services *as well as business services* across lines of business and jurisdictions will require transforming how state government acquires and manages these services. Currently, state government employs processes for procurement, budgeting, funding, and project management that are put in place to primarily accommodate capital investments in IT capabilities that will serve a particular agency. States have been emphasizing an *enterprise perspective* regarding IT services and business services for some time. States are now exploring approaches for delivering IT services that can be characterized as *inter-enterprise* and *multi-jurisdictional*. This requires states to employ new processes for evaluating, acquiring and managing IT services that may be purchased from an outside service provider that involve no capital investment. This doesn't mean that there will be no capital investments. Rather, the aforementioned processes must be examined and potentially re-engineered to include additional candidate paths for employing internal and external IT services.

Final Thoughts

There is story of a well known furniture company with a reputation for producing high quality furnishings. Early in its history it managed its entire supply chain including feedstocks, design, manufacturing, product management, sales, delivery of goods, and customer care. In the last decade this company has embraced the new service economy. One change is that delivery of furniture is done by contracted independent shippers. Whereas its own employees had delivered furniture to the customer with the utmost care due to a sense of ownership, the new independent shippers are only concerned with getting "materials" from point A to point B as quickly as possible. Furniture that was once carefully wrapped and secured within well maintained trucks is now packed as tightly as possible with auto parts, hardware store merchandise, liquids, and whatever else the shipper can include in a load using a *rented truck*. Furniture that once arrived without a mark, a finger print, a smudge, or oil and grease marks, is now scratched, gouged, abraded, even broken. What happened?

As government engages more and more external services, it must maintain ownership for the outcomes achieved. Concern and care for citizens can not be contracted. In order to mitigate the disparity between a dedicated government public servant and a contractor, contracts and service level agreements must be detailed sufficiently to get as close as possible to a the behavior of a dedicated public servant. Is that possible? Sometimes it is. Understandably, the primary motivation of a service provider is profit. The motivation of a public servant is public service. What is needed in these circumstances are suppliers who are motivated by profit *and* public service.

Government policy makers, officials, professionals, and employees must remain vigilant of the mission of government and ensure citizen outcomes are achieved as *effectively* and *efficiently* as possible. Efficiencies can be so emphasized and pursued that effectiveness is compromised. Service orientation is an approach to reducing costs. Government must ensure that proper care and concern are not compromised in the process. This is a significant challenge in today's economy. Further, there are government services that should not be delegated to an external service provider. Over time, we will all learn, make course corrections, mature, and become more judicious is what government business and IT services are moved to external providers. Be prepared for surprises, failures, and great successes. But don't presume external service providers or cloud computing will be appropriate under all circumstances, or will necessarily deliver state government out the current economic crisis.

The Ponemon Institute conducted two surveys related in cloud computing. In May of 2010, Ponemon Institute published *Security of Cloud Computing Users*. In April of 2011, it published *Security of Cloud Computing Providers Study.*[28] Conclusions from these studies include:

- The majority of cloud computing providers surveyed do not believe their organization views the security of their cloud services as a competitive advantage. Further, they do not consider cloud computing security as one of their most important responsibilities and do not believe their products and services substantially protect and secure the confidential or sensitive information of their customers.

- The majority of cloud providers believe it is their customer's responsibility to secure the cloud and not their responsibility. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers.

- Buyer beware – on average providers of cloud computing technologies allocate 10 percent or less of their operational resources to security and most do not have confidence that customers' security requirements are being met.

Further, the majority of the cloud providers that participated in the Ponemon study admit they do not have dedicated security personnel to oversee the security of cloud applications, infrastructure or platforms.

Calls to Action for the state CIO.

- Evaluate cloud computing as an alternative approach for delivering IT services.
- Establish the entrance criteria for considering cloud computing as an option for delivering IT services.
- Examine the impact of cloud computing on federal programs that are administered by the states. Understand the program, legal and policy issues related to the inherent characteristics of cloud computing such as multi-tenancy, and sharing services across government lines of business.
- Develop a cloud computing strategy and evaluation process that involves enterprise architecture, security, records management, procurement, legal, and other expertise centers as appropriate.
- Manage cloud services within the portfolio of government IT services.
- Ensure that business processes are working efficiently and effectively before applying technology to support them.

Contributors

Patricia Cummens, Account Executive, ESRI

Paul Warren Douglas, Enterprise Architect, State of Washington

Scot Ellsworth, Chief Enterprise Architect and Director of the Office of Enterprise Architecture, State of Michigan

Lauren Farese, Public Sector Senior Director, Oracle

Mike Fenton, Director of Enterprise Architecture, State of North Carolina

Jeremy Foreman, Public Sector Enterprise Architecture Program Director, Oracle

Sam L. Hearn, Jr., Graphic Designer, AMR Management Services

Bob McDonough, Chief Cloud Architect, State of Michigan

Andris Ozols, Chief Policy Advisor, State of Michigan, Department Technology, Management and Budget

Doug Robinson, Executive Director, NASCIO

Bill Roth, Chief Information Technology Architect, State of Kansas

Shawn K. Vaughn, Membership & Communications Coordinator, NASCIO

Appendix – References

The Australian Government Cloud Computing Strategic Direction Paper
http://www.finance.gov.au/e-government/strategy-and-governance/docs/final_cloud_computing_strategy_version_1.pdf

The Department of Finance and Deregulation, through the Australian Government Information Management Office, has consulted with government agencies, industry and the public to develop an Australian Government Cloud Strategic Direction.

Cloud Computing Use Cases Group (Google group)
http://groups.google.com/group/cloud-computing-use-cases

This group is devoted to defining common use cases for cloud computing.

Computer Crime & Intellectual Property Section, United States Department of Justice
http://www.justice.gov/criminal/cybercrime/ssmanual/

The purpose of this publication is to provide Federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations. Chapter 3 of this publication presents the Stored Communications Act (SCA). The significance of the SCA is that it imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

Cloud Customers' Bill of Rights
Information Law Group LLP – www.infolawgroup.com

The InfoLawGroup has issued a "Cloud Customers' Bill of Rights" to serve as the foundation of a cloud relationship, allow for more transparency and enable a better understanding of potential legal risks associated with the cloud.

Detailed descripton of the Cloud Customers' Bill of Rights
http://www.infolawgroup.com/2010/10/articles/cloud-computing-1/cloud-computing-customers-bill-of-rights/

The Cloud Security Alliance (CSA)
https://cloudsecurityalliance.org/about/

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Aliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Federal Cloud Computing Strategy
http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

This Federal Cloud Computing Strategy is designed to:

- *Articulate the benefits, considerations, and trade-offs of cloud computing*
- *Provide a decision framework and case examples to support agencies in migrating towards cloud computing*
- *Highlight cloud computing implementation resources*
- *Identify Federal Government activities and roles and responsibilities for catalyzing cloud adoption*

The Jericho Forum (The Open Group)
http://www.opengroup.org/jericho/

Jericho Forum is the leading international IT security thought-leadership association dedicated to advancing secure business in a global open-network environment. Members include top IT security officers from multi-national Fortune 500 companies and entrepreneurial user companies, major security vendors, government, and academics. Working together, members drive approaches and standards for a secure, collaborative online business world.

The Fiscal Survey of States - National Association of State Budget Officers
www.nasbo.org

The Fiscal Survey of States is published twice annually by the National Association of State Budget Officers (NASBO) and the National Governors Association (NGA). This survey presents aggregate and individual data on the states' general fund receipts, expenditures, and balances.

Spring 2011 Fiscal Survey of The States – Summary
http://www.nasbo.org/LinkClick.aspx?fileticket=IW3fw0p2k0A%3d&tabid=38

Spring 2011 Fiscal Survey of The States – Full Report
http://www.nasbo.org/LinkClick.aspx?fileticket=yNV8Jv3X7Is%3d&tabid=38

National Institute of Standards and Technology Cloud Computing Program
http://www.nist.gov/itl/cloud/index.cfm

The long term goal of this program is to provide thought leadership and guidance around the cloud computing paradigm to catalyze its use within industry and government. NIST aims to shorten the adoption cycle, which will enable near-term cost savings and increased ability to quickly create and deploy enterprise applications. NIST aims to foster cloud computing systems and practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios.

The Open Cloud Manifesto
http://www.opencloudmanifesto.org/

Dedicated to the belief that the cloud should be open. This effort intends to initiate a conversation that will bring together the emerging cloud computing community (both cloud users and cloud providers) around a core set of principles. We believe that these core principles are rooted in the belief that cloud computing should be as open as all other IT technologies.

---

[1] Michael Hugos and Derek Hulitzky, *Business in the Cloud, What Every Business Needs To Know About Cloud Computing* (New Jersey: John Wiley & Sons, 2011), pp 1-20.
[2] The Federal Cloud Computing Strategy. Available at http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf.
[3] National Institute of Science and Technology Working Definition of Cloud Computing. Retrieved from http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html. See also Cloud Computing Security Alliance (CSC) *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,* p. 14.
[4] The NIST Definition of Cloud Computing, Authors: Peter Mell and Tim Grance, Version 15, 10-7-09. See http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html. These definitions are republished in multiple reference documents including the CSC publications.
[5] *Business in the Cloud, p. 44.*
[6] *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, ISACA, 2010. Retrieved on May 10, 2011, from https://www.isaca.org/search/Pages/ResultsAjax.aspx#cloud%20computing. Additional input from interviews with state and corporate members of NASCIO.
[7] *Business in the Cloud, p. 44.*
[8] *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, ISACA, 2010. Retrieved on May 10, 2011, from https://www.isaca.org/search/Pages/ResultsAjax.aspx#cloud%20computing.
[9] *Business in the Cloud, p. 44.*
[10] *Input from interviews with state and corporate members of NASCIO.*
[11] *ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2010.
[12] *ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2010.
[13] *ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2010. Additional input from interviews with state and corporate members of NASCIO.
[14] *ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, 2010.
[15] Cloud Computing Security Alliance (CSC) *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,* p. 18.
[16] Gartner Global IT Council on Cloud, June 2010
[17] *Executive's Guide*, p. 183.
[18] *Executive's Guide*, p. 179.
[19] *Executive's Guide*, p. 180.
[20] *Executive's Guide*, p. 181
[21] NARA Bulletin 2010-05, retrieved on March 2, 2011, from http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html.

[22] *IT Governance and Business Outcomes – A Shared Responsibility between IT and Business Leadership,* p.2. Available at www.nascio.org/publications.
[23] The NASCIO Enterprise Architecture Value Chain is presented and described in multiple NASCIO publications including the NASCIO Enterprise Architecture ToolKit, NASCIO series on analytics and transformation. These publications are available at www.nascio.org/publications.
[24] *Executive Guide*, p. 134.
[25] *Business in the Cloud, p 1. The Nature of the Firm by published in 1937 by Nobel Laureate, Ronald Coase,.*
[26] *Council of State Governments, National Center for Interstate Compacts, FactSheet. p. 1. Available at http://www.csg.org/programs/policyprograms/NCIC/NCIC_resources.aspx.*
[27] *Multi-State GIS Cloud Services Assessment Team RFI Response Assessment, Business Case & Recommendation.* Retrieved from http://itsd.mt.gov/content/policy/councils/mliac/March_2011/GIS_Cloud_Computing.
[28] *Security of Cloud Computing Users*, April of 2011; *Security of Cloud Computing Providers Study,* May of 2011. Poneman Institute. Retrieved on May 12, 2011, from http://www.ponemon.org/index.php.

This project was supported by Grant No. 2010-DJ-BX-K046 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author.