NASCIO
Representing Chief Information Officers of the States

NASCIO Cloud Computing Series

Capitals in the Clouds

Part III – Recommendations for Mitigating Risks: Jurisdictional, Contracting and Service Levels

NASCIO Staff Contact:
Eric Sweden
Program Director,
Enterprise Architecture & Governance
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

Cloud computing is here to stay and will grow

Based on one recent national survey of state CIOs, cloud computing is an essential ingredient of a cost saving recipe for state government. Adoption or planned adoption is almost universal and growing.[1] NASCIO's earlier briefs in this series provided foundational concepts and discussed data management issues related to cloud computing. Cloud computing, or the sharing of resources across the state government enterprise, offers the promise for significant savings, operational efficiencies, and reduction in IT capital investment. All of the benefits of cloud computing are exploited further as state governments begin to create interstate collaboratives that join state government enterprise operations. Collaborative models involve state and local government, federal/state/local government, and even international collaboratives. Such collaborative efforts will only increase, and the rationale for these collaborative efforts are fairly obvious. Not only as cost saving and cost elimination efforts, but also from a "connectedness" perspective – something government has been desperately trying to achieve within homeland security, law enforcement and first responder community for the last decade.

This issue brief will continue the exploration of some of the key issues, components and potential solutions that should be included for consideration in evaluating and planning for cloud services. Key considerations include:

- multi-jurisdictional enterprise architectures
- innovations for optimizing government investments and services

- jurisdiction issues
- statutory assertions
- contracting issues
- service level agreements
- policy and governance issues
- data considerations
- opportunities for optimizing business operations across jurisdictions

Even as multi-agency, multi-state, multi-government collaboratives are being evaluated, designed and implemented, there are considerations that must be dealt with head on. NASCIO's Part II in this series highlighted *data management* issues. Part III highlights what can be termed *jurisdictional, contracting and service level* issues. Such issues do not preclude utility computing, multi-jurisdictional collaboratives and shared business processes. However, the complexity of the legal environment, the data environment, human capital, operations, finance and accounting require the development, and implementation of appropriate *new operating discipline*. That operating discipline essentially constitutes the enterprise architecture or an *aggregate enterprise architecture* which will include governance, economics, human capital, business processes, information and knowledge management, and operations management that will enable the delivery of common IT and business services intent on serving the citizens effectively and efficiently.

New government operations will include a portfolio of organization and process architectures that will need to be evaluated and selected based a number of parameters. These parameters include but are not limited to the following: the strategic intent of state government and local government(s) that are now going to share resources; number and complexity of the organizations that intend to come together; relevant statutes and regulations that govern the behavior of the constituent parties. The greatest challenge will be the organizational change from what have been fairly autonomous government entities to a *network* of government entities that are now sharing responsibilities, business and technology capabilities, and funding to orchestrate the delivery of government services. Cloud computing is one of the technology capabilities that will enable this *transformation*.

Cloud computing is a technology strategy that enables more than simply optimizing computing utilities. It enables strategies for *optimizing government business services,* and achieving *new levels of orchestration* of government services across a state, a region and even nationally.

Know What You Are Getting Into

State government continues to explore innovations for optimizing and harmonizing IT services across state government. Potentially, government business services as well. There are multiple cloud computing deployment models ranging from internal private clouds to government community clouds to government *line of business* community clouds to public clouds that are external to state government. As government explores its options, and the various scenarios for engaging cloud computing services, consideration must be given to a number of issues. These include, but are not limited to the following.

- *Actual total cost of a service*
- *User fees / access fees*
- *Exit strategy / switching strategy*
- *Potential for data breach*
- *Legal liability – assigned and assumed*
- *Service provider's access and use of government data – including emails and the content of email attachments*
- *Provider's economic model for pricing which may include reselling government data, or reselling analytics about the data*
- *Physical location of the data and applications*
- *Jurisdictional issues related to the physical, virtual, and legal location of data and applications*
- *Proximity to and threats from other data tenants – intended and unintended*
- *Risks associated with the multi-tenant or multiplexing physical infrastructure environment*[2]
- *. . . the list continues to grow . . .thus the need for agile, dynamic enterprise architectures*

NASCIO has been working with its government and industry members to develop a *list of considerations* for cloud computing. It should come as no surprise, the list continues to grow. The most significant issues are really centric on the public or external end of the spectrum of cloud deployment models. Internal clouds and external private clouds remain the most stable and controlled environments for state government. These *internal* models have been around for some time, though they have been called different things. State government has been working on consolidation, shared service, and optimization models that rationalize IT services. Moving away from this "internal" model requires significant evaluation of not only the immediate issues, but also secondary effects of these issues. As stated in NASCIO's series on analytics – there are *secondary and tertiary effects* of any decision that may erode the value originally assumed.

Sharing of resources is a strategy for dealing with the "new normal"

- ***Multi-jurisdictional enterprise architecture***

NASCIO has defined enterprise architecture and created a graphic to describe the concepts of enterprise architecture at a high level – the *NASCIO Enterprise Architecture Value Chain*.[3] The NASCIO definition and the value chain are relevant within the current circumstances. And, it is the discipline of enterprise architecture that governments (state, local, federal) will need to apply in the planning, evaluation, design, implementation and maintenance of collaborative government initiatives and operating models in areas such as human services, transportation, health, environment, economic development, and public safety.

The importance, value and inevitability of collaboratives is demonstrated by NASCIO's creation of the State and Local Collaboration Working Group in 2011 under the auspices of the *Enterprise Architecture and Governance Committee* to inventory, assess and promote state and local government collaboration of IT initiatives, shared services and common solutions. As stated in previous issues

in this series, the western states' alliance brings together a diverse membership of states to share GIS data storage capabilities. Several groups of states have formed regional consortia to share IT and business services related to unemployment insurance (UI) claims processing. It can be expected that states will come together into a variety of collaboratives in other lines of business as well.

- ***Anticipate, prepare and execute***

Multi-state collaboratives by necessity entail *multi-jurisdictional* issues. In order to create such arrangements successfully, the inherent issues and inevitable collisions in policy, legislation, economics, data management, operations and human capital must be anticipated and accommodated through multi-jurisdictional enterprise architectures that include all elements of the aforementioned operating discipline. NASCIO will systematically address these issues and develop calls to action, inventory best practices, explore frameworks and operating models, present case studies, and develop a roadmap for successful collaboratives. Such arrangements are complex. That complexity will need to be managed and orchestrated through proper governance that employs multi-tiered frameworks and methodologies for organizing a host of government resources.

The focus of this issue brief is on some of the *jurisdictional issues* associated with cloud computing with an emphasis on public cloud deployment models. Also discussed are some of the issues that eventually *lead* to the question of jurisdiction. Again, these issues are most relevant within the *public cloud* and *multi-jurisdictional community cloud scenarios.*

Internal cloud scenarios *shield* state government from jurisdictional issues. Internal clouds that are created and provisioned by state government staff constitute efforts for optimizing state government IT services within a state. Internal deployment models provide economies of scale, and provide the same level, or higher, security provisions state government has provided in the past. Internal, or private clouds, are a first choice for state government to avoid many issues related to security, jurisdiction, data ownership, data integrity, disaster recovery, and trust.

Due to economic pressures, state governments are evaluating cloud deployment models that entail a combination of private, hybrid, and public cloud scenarios. It is the *public cloud scenario* that requires the highest level scrutiny relative to the aforementioned list of issues. When these issues are on the table, some external cloud providers may find the *economies of scale* that allow them to offer highly competitive pricing begin to diminish. This will then potentially erode the competitiveness of some external cloud offerings as compared with internal cloud offerings. On the other hand, some cloud providers will seize the opportunity to create the means for enabling multi-jurisdictional collaboratives by providing the necessary infrastructure, security, vetting of personnel, service availability and data integrity that will meet the statutory requirements of state government terms and conditions and still achieve *economies of scale* that will ensure *economic profitability.*

Some community cloud offerings may provide a *better* model for external cloud providers and their customers to achieve dramatic economies of scale while

meeting common requirements for a cohort, or community, of customers. In this scenario, the jurisdictional issues are still of great concern. It still matters, WHERE the data resides physically, the *level of separation* of that data from other data tenants, and WHO has jurisdiction over that data. However, as society, government and industry mature in the development of collaborative models for organization, economics, operations and logistics, and service delivery; the legal environment will be challenged to keep up and accommodate the demand for optimization efforts.

Understanding the Risks

We've dealt with some of these in past briefs, and we'll systematically address others.

- ***What are the risks?***

Data is the *currency* of government and it must be protected. Possibly the most critical data is employee and citizen personal data particularly personally identifiable data (PII). *Appendix A presents examples and discussion of PII.* Another valuable data resource is *secondary data* that can be used to *derive* PII. This same data must also be protected in or out of a cloud services environment. State government must be cautious when moving this data into *non-private* clouds. In certain types of cloud deployment models, state data may be stored in a multi-tenant environment. Some multi-tenant environments may also house data from a variety of economic sectors, industries, governments and jurisdictions. This is the case where cloud providers are offering *commodity services* to a broad customer base with little or no connection to the optimization efforts of government collaboratives.

In the case of the formation of a *multi-jurisdictional collaborative*, data may also reside in a multi-tenant environment, but the cohort of tenants are from the same economic sector – government, industry, non-profit, or academic; or line of business – e.g., justice, transportation, human services. In any of these scenarios, there is the potential for data breach, data corruption and other threats that result in harm.

The loss of PII or derivatives can trigger litigation. It is through the due process of law - that is, the process of litigation - that jurisdictional issues will become relevant. A court then must determine if it *has jurisdiction* over a service provider, or the property in question. Jurisdiction is essentially the *authority* of a court to *hear and decide* a specific legal action.[4]

Risks associated with some cloud computing scenarios which can trigger disputes and litigation include but are not limited to the following:

- *data protection and privacy*
- *sharing data residence with other service provider customers*
- *outright theft of data*
- *hackers*
- *unintentional release of data*
- *sending, storing, processing of data in multiple jurisdictions*
- *censorship*

- *computer crime*
- *contracts*
- *copyright*
- *defamation and libel*
- *discrimination*
- *fraud*
- *harassment*
- *intellectual property*
- *taxation*
- *trade secrets*
- *trademark*
- *inter-tenant data penetration, corruption, modification*

State government has had to be concerned about privacy, security, e-discovery requests, and disaster recovery in the past, so there is nothing new in terms of those issues. In a multi-tenant environment, state government must also be concerned about the events and circumstances of the *other* tenants. What happens to and through other tenants can have an impact on state government if it is also a tenant. Good *risk management* necessitates that state government conduct due diligence to *anticipate* potential events, and *evaluate* the probability of and the outcome of such events and the ultimate effects on state government and its citizens. This train of thought then surfaces the jurisdictional issues discussed in this issue brief.

- ***Jurisdictional issues***

As stated in NASCIO's *Capitals in the Clouds, Part II*, there are necessary steps in the process of "evaluating" cloud computing, *as well as other shared resource approaches*, for achieving optimization and reduction in redundancy. State governments need to *continually evaluate* the issues that arise with cloud computing. Some issues have not been anticipated – *there will be surprises*. It can be anticipated that cloud computing strategies must include consideration for *data issues, jurisdictional issues and human resource issues*. These are not simple issues. Specifically, state governments need to be considering the following relative to cloud computing services:

1) STRATEGIC INTENT associated with employing cloud computing services. What are the outcomes sought for pursuing such a model? Clear, explicit strategic intent will guide portfolio choices for enterprise architecture related to collaboratives.
2) LOCATION of data and applications. Where are state government data and applications stored and maintained geographically *and legally*?
3) RELEVANT STATE LAWS that provide parameters on what a state can and can't do in terms of *joining* other governments. Joint powers authority and the laws of potential partner governments provide parameters for candidate government partners to evaluate from their individual stance the possibility and statutory limitations associated *joining* other governments as well any other enterprises. State laws also specify *terms and conditions* that service providers must meet in order to comply with statutory requirements.
4) CONTRACTUAL PROVISIONS contained in s*ervice provider terms of service*, that are explicitly prescribed in a contract, *or are assumed*, in a contract with a service provider.

"With states facing continuing fiscal turmoil, one might expect to see a mass migration of state IT services to the cloud in an effort to produce cost savings."[5]

As stated in NASCIO's previous issue briefs in this series, the issues encountered with cloud computing are not necessarily new issues. These same issues are present in other shared resource scenarios. Cloud adoption is accelerating and brings a new emphasis to these issues. What is driving state government toward cloud computing and other resource sharing strategies is *cost reduction*. The pressure for cost reduction is driving states toward evaluation of various collaborative, or shared services approaches. The scope of consolidation or optimization efforts can involve two organizations, or fifty. For example, optimization initiatives can vary in scope.

1. Agency only
2. Multi-Agency
3. Multi-jurisdiction within a single state that include counties and cities
4. Multi-jurisdiction communities across states

Collaboratives, or shared services models seem to be simply an application of common sense from an operational perspective. The basic functions of government from state to state are so similar that it only makes sense to develop *common IT solutions* as well as *common business solutions*. In bringing together multiple states, or multiple jurisdictions, the individual governments begin to examine the risks as previously outlined. That evaluation of risks may trump the rationale from an operational perspective. Much of the risk assessment for forming collaboratives acknowledges that state government is breaking new ground that goes beyond historical collaborative initiatives, and the patterns that already exist in interstate compacts involving borders and interstate policy issues. In fact, *the new driver* for cloud computing is more of an emphasis on *business operation efficiencies and optimization* rather that than merely trying to achieve IT cost savings.

When we begin looking at number 4 – *multi-jurisdictional communities* – particularly in the virtual world, we are facing a whole new level of issues related to jurisdictional authority. Jurisdictional issues related to cloud computing are *emerging*. There are unique situations that are surfacing for the first time. Further, oftentimes there is no existing case law for these situations that can be referenced. Legal precedent has not been established for conflicts involving multiple jurisdictions related to customers and service providers in a multi-tenant cloud environment, particularly when that virtual environment is fragmented across a diverse physical geography. It can be expected that case law *will* emerge and it can be anticipated that in the future, courts will rely on early case law that has set precedent. Therefore, it is critically important to establish the *right precedent* and *the rationale for such precedent* in the early cases that arrive. Anticipation of and proper provisioning for potential, perceived, and real jurisdictional conflicts on the forward side of contract negotiation and multi-jurisdictional collaboratives, can avoid some conflicts, and help mitigate others. As with any organization, the enterprise architectures for multi-jurisdictional organizations must be agile, fluid, and adaptable as new situations and challenges arise.

There are many unknowns – whose laws apply?

Cloud computing, particularly, public cloud deployment models, are promising significant savings achieved through *economies of scale*. This message is extremely attractive to state and local governments facing a *historical and persistent budget crisis*. The legal and jurisdictional issues related to public, or external, cloud offerings are *future issues*. *They haven't arrived yet*. Legal precedent has not been created yet. Contracts, service level agreements, provider terms of service, state government terms and conditions, and disclaimers related to cloud computing have not been tested in courts. Further, federal laws apply to *all* states and territories. The laws of a particular state apply to *that specific* state. The collision point of conflicting state laws and contract terms and conditions is what presents the greatest concern. And, the outcome is unknown.[6]

Further, without proper evaluation of cloud alternatives, particularly contracting, state governments and cloud suppliers may find themselves in courts more times than not. It should be anticipated that jurisdictional issues related to cloud computing will involve *multiple* jurisdictions, and therefore, *multiple* courts.

What courts will have jurisdiction to decide cases?

What cases will arrive?

What is a Court to do? Does Anyone Know?

Much of the legal precedent is yet to be established. It may be that a court will decide that cloud providers are *assuming* responsibility for knowing the applicable state government legal requirements, statutorial terms and conditions, and the implications associated with servicing customers residing in multiple jurisdictions. Or, a court may decide that state government and state government employees assume responsibility for knowing the terms of service presented by cloud providers and therefore cannot transfer certain responsibilities or risks to the primary cloud provider.

State governments are grappling with jurisdictional issues, the potential for court orders being issued from a court in one state to officials in another state, and the high potential for questions of jurisdiction when data from a state government physically resides on foreign soil. These issues are examples of governance and risk management issues that must be thought about, discussed and resolved prior to state government committing to certain cloud computing scenarios. These are complex issues of jurisdiction that cannot be adequately resolved once a state government is facing court orders from an out of state court, or a court in another nation. They have to be considered and dealt with in advance. It should be anticipated that court orders may be issued for the release of information, the release of encryption keys, or for government officials and employees to appear in court. "Courts" may be foreign as well as domestic courts. These courts may be exercising common law or statutory law. In common law cases, courts will rely on or be creating precedence. Statutory law will specify how the law is to be applied and leave little room for interpretation. The associated costs of dealing with these situations can entail significant financial burden to state government.

The Service Level Agreement Protects Us! . . . Really?

- Do you think that, or do you know that?
- Do you assume a provider is promising to protect your data? Or, are they planning to exploit your data? Is access to government data essentially part of the consideration received by the cloud provider?
- Is your service level agreement balanced, or is it one sided? Has such an agreement been properly reviewed by legal staff?
- Do government employees understand the implications for state government when they create a cloud account, or "click through" and accept a service providers terms of service?

At the start of this discussion, it must be understood that service level agreements (SLAs) are not adequate and cannot be adequate for *actually* protecting citizen's identity, and privacy. Nor can SLAs be constructed to prevent data breaches, seizure of data bases, or other actions that threaten government data assets. These signed agreements are put in place to motivate service providers to put necessary safe guards in place.

- ***What constitutes "reasonable effort"?***

The terms "reasonable effort", or "reasonable security" are used in many federal and state security regulations – but what constitutes "reasonable effort?" The meaning of that term becomes debatable without clear definition. Reasonable effort then should be clearly defined and constitute a minimum requirement for security. Contracts should state that the cloud provider will maintain *reasonable* security capabilities to:[7]

  - protect information from unauthorized access, use, alteration, or disclosure
  - protect and ensure confidentiality, integrity and availability
  - prevent breach, and malicious code infection

What constitutes "reasonable security" will be an ever moving target as technology capabilities continue to develop and mature, and the financial feasibility of employing these capabilities increases.[8] Further, a service provider may have adopted a position of *economic non-compliance*. In other words, it may be more economical to be in non-compliance and pay the financial penalty rather than incur the necessary costs of true compliance. That shouldn't surprise anyone since the push for cloud computing is typically anchored in economic models intended to drive down cost. This discussion highlights the essential need for independent, repeated audit of cloud provider services and operations.

- ***What a contract or service level agreement cannot do***

Once data is stolen, mishandled, or released, it cannot be retrieved. It will be exploited by criminals for the criminals' advantage with *no concern* for citizens or the outcomes that citizens will have to live with. State government must evaluate service offerings with their eyes wide open. Cyber criminals are tenacious and relentless in their pursuit of opportunities for accessing, retrieving

and selling information. However, as presented in Part I of this series, many cloud providers do not consider it to be their responsibility to actually protect customers' data.

There are inherent risks associated with cloud services. The greatest risk exists with external or "public" cloud services. In theory, cloud computing or resource sharing can provide economies of scale that can drive down the cost of IT services. Many of these economies of scale, particularly with an external provider, are based on certain assumptions and the characteristics of cloud computing that combine to present the often touted *variable cost*. That variable cost increases as new capabilities and requirements are added.

"Buyer Beware" is excellent advice for state government as it evaluates cloud computing options.

- ***Beware Self Provisioning***

One of the promises of cloud computing is rapid provisioning – rapid elasticity. If that provisioning is triggered through the process of an employee or agency engaging a cloud service, or through a "click-wrap" agreement, then the state has no opportunity to negotiate terms of service. Without that negotiation, the cloud provider may not have contractual responsibility for data security, data quality, privacy, availability or other performance issues.[9]

There may be an additional spin on some of the terms of service. Not only may the service provider *not* provide any assurances of protecting the customers' data, they may boldly state that they will scan it, exploit it, re-package it, and resell it at their own discretion. A cloud services, or shared services provider, may have a packaged price that is based on their assumption that the data resource they are storing provides additional value to them for data mining purposes. Such may be factored into the economics of their pricing model. Depending on the terms of service, the provider may assume *ownership* of the data. The provider may go further in this progression to charge the customer "access fees" for any access by the customer to the customer's data. *Note: it is the customer's data from a reality perspective, but it may be provider's data from a legal perspective*. These fees that may not have been apparent on the front end of such arrangements. This progression continues - if the customer wishes to switch providers, there may be additional and potentially significant fees to retrieve a "copy" of the data. Even then, the cloud provider may claim that they "own" the data in their possession, and it will remain in their storage for their use. The question is, "who would agree to such one sided terms?" Probably no one if they read and understood the provider's terms of service. Additionally, how would citizens react if they knew that such situations exist?

State government employees, acting knowingly or unknowingly as "agents" of state government, that engage cloud services without proper legal review may be putting their state and themselves into a high risk, and potentially a high liability situation. Coming in toward center from that extreme may entail brief negotiations or evaluations focused on the *technical capabilities* of an IT service with only a cursory review of the service provider's terms of service. This can lead to the situation described earlier where government agencies have unknowingly signed over ownership of their data to the IT service provider with-

out knowing what "ownership" means. Subsequently, the agency must seek permission to access that data. This scenario not only entails economics, data ownership, data integrity and security, it can also compromise state government's ability to impact public health and public safety when data and information access are inhibited, or delayed due to required provider permissions and transaction costs associated with information requests.

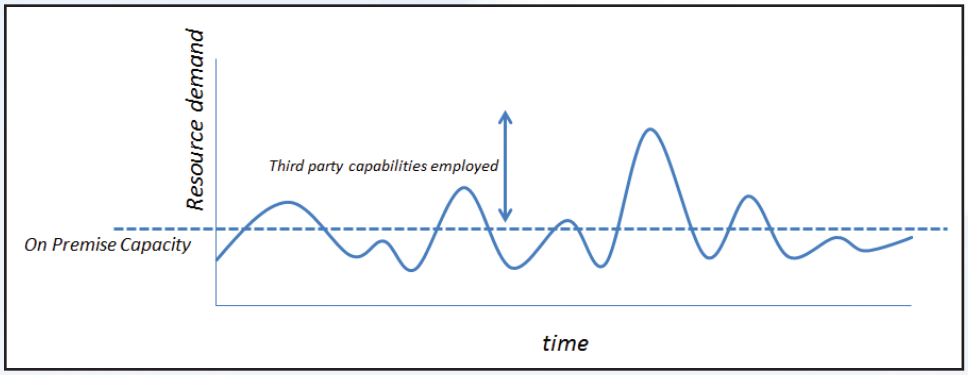
It is important to review existing security policies and update them as necessary to preclude unauthorized creation of cloud accounts. This includes "free" accounts. It is just as necessary to build awareness of the risks and potential liabilities related to such accounts.

Evaluating Cloud Providers - It Is Not Just About Operations

Evaluations of service capabilities may even be extensive from an operational perspective. However, review of the considerations related to jurisdiction, security and privacy, may dwarf technical reviews due to the complexity of the laws and the potential *conflicts of laws* that exist.

These considerations must be included in requests for information (RFI) and request for proposal (RFP). As these considerations are recognized and discussed, provisioning for these considerations will begin to reshape, potentially erode much of the economies of scale that were initially justifying the move to the cloud services or shared services alternative.

Cloud computing, particularly public clouds are not appropriate for some applications and certain types of data. Cloud computing is characterized as potentially employing resources from anywhere in the world. There is the opportunity to exploit or leverage computing resources such as storage, processing, applications, and technical infrastructure from *third party providers* who may be located in any state or territory, as well as any continent. The provisioning of any resource need can come from any number of sources and involve different *third party* service providers depending on the current cost of *computing commodities* and the sourcing decision of the primary cloud provider. This "commoditization" of resources is one of the ingredients of cloud that make it profitable for the primary cloud provider. Rapid elasticity is one of the necessary five characteristics of cloud computing. Sometimes this is termed *agile capacity provisioning*. Cloud providers can often meet this characteristic by employing third party resource providers *temporarily*.



Elasticity of Demand

One way to mitigate or avoid potential issues related to this concept of *elasticity and third party providers* is to include contract provisions that require that any third party providers employed by the primary service provider *must provide* services at the same level of performance and within the same terms and conditions established with the primary service provider. The primary service provider is *guaranteeing* rapid elasticity. This requires that they *can be agile* in employing additional resources on an as-needed basis. The primary provider must then identify and engage strategic partners so they are in place *in advance* with the additional requirement that these partners are subject to the same service level agreements, and terms and conditions for the each of the relevant communities served. There will be contracting and service portfolio issues for both the primary provider and third party providers. In other words, the primary provider will need to guarantee that third party providers are *capable* of providing services to the various communities the primary provider serves. The question is, can they? Are such provisions included in the contract and is compliance with these provisions verified? Even if such provisions were in place at the time of a data breach, what remedies are possible particularly when third party providers are in a foreign country? This then may entail a next level of audit – verification and validation of third party service provider services. This will then have a necessary impact on the pricing of the primary cloud provider's services as well as the third party providers.

Complications, Complications! – Whose Terms and Conditions Will a Court Apply?

Cloud computing is a new wave in computing which brings with it new issues, and possibly many of the same issues but on a different scale. Data breaches, for example, have occurred in past in non-cloud scenarios. However, in a cloud computing scenario, particularly a public cloud, the potential magnitude can be greater, depending on a number of factors including the number and types of tenants in a multi-tenant cloud environment. Depending on how many "layers" of third party contractors, the jurisdictional issues can become extremely complicated. There is the issue of whose laws apply in any litigation that may occur. Further in a multi-tenant scenario, there is the question of whose terms and conditions will be applied by the court.

A court or jury may apply the most stringent terms in judging a consolidated litigation case involving multiple tenants regardless of the disparities in "signed" agreements.[10] Precedence will eventually be established for common law courts absent regulations or statutory requirements. Additionally, in questioning whose laws will prevail, or will be applied, the answer may be – *all of them*. In other words, in the case of a data breach, and/or a case of non-performance, the case may be tried in multiple courts and result in multiple decisions and penalties. Notwithstanding the loss of citizen data and the associated personal loss on the part of citizens, primary cloud providers and particularly those that employ third parties may themselves be facing significant financial risk.

Location! Location! Location!

If data is physically stored in certain foreign countries, the domestic law of those nations would apply to information stored on servers in that country regardless of whether such foreign storage was prohibited by the cloud vendor's contract or SLA. Once the data resides on that soil, within that jurisdiction, it is subject to the sovereignty of that nation's laws. *It doesn't matter that it wasn't supposed to be there*. This same jurisdictional issue may exist if data is *transmitted* on a foreign owned telecommunications network.

Several state Attorneys General have expressed concern regarding the storage of sensitive data collected by their states on servers *outside* the state. Not only do they not want their data maintained on foreign soil, they don't want it maintained in another state within these United States. States indeed have a challenge that is particular to state governments. Federal law applies throughout the nation and carries with it application in *every* state and territory. However, the laws of a *specific* state only apply to *that* state. State A law only applies to *State A*. State B law only applies to the *State B*. There is, in fact, a legal field focused on "conflicts of laws", that attempts to rationalize the issue of conflicting jurisdictions when the court of one state can and should apply the law of another state. However, this is a highly complex legal specialty and it is best to avoid this conflict. *(See Appendix C)*

According to Gartner, most laws do not relate to the *physical location* of data. Rather, they relate to the *legal location* of data. A court may interpret the physical location of the data as irrelevant. In other words, in certain situations, the legal entity that holds the data determines what a court will consider as the "location" of data — and not the physical location of the server, the citizenship of the individual or the physical location of data collection. Where the cloud service provider and the organization that consumes cloud services are legally registered in the same jurisdiction, companies have taken the position that there is no legal problem, because the contractual obligations can be enforced locally. In some cases, organizations have already signed contractual agreements with their clients to store data locally. However, this severely limits the choice of cloud deployment models these organizations can employ.[11]

Restrictions such as physical location of data that are stipulated in service level agreements and contracts should be evaluated and constructed based on the *nature and sensitivity* of the data and information being stored. Such restric-

tions will also be employed simply to avoid *conflicts with laws* of other jurisdictions. Terms of service can be an issue even with services other than cloud computing services. The provisions of service level agreements have now become a significant issue because of the anticipated level of adoption of cloud computing services.

As states are actively pursuing cloud computing alternatives, they must anticipate and prevent the occurrence where a litigant appears in another state's court with an e-discovery request based on the fact that a given state's data is housed in another state's location. States should avoid litigation in a court outside its borders even if that outside court applies the laws of the state that "owns" the data assets. This occurrence will necessarily involve "conflicts of law" and potentially burden states with egregious fees related to legal fees, travel, research, and the expected escalation to appellant courts. State budgets are tight and cannot accommodate this unnecessary litigation.

Encryption of at-rest state data that is located in another state does not solve this issue. Even though readable data might not be vulnerable to immediate, intelligible seizure, the legal issue still remains. Encryption only adds another layer of litigation. *(For example, Judge of State A: "Now that I have granted your e-discovery request for State B data stored here, I will hear the issue of ordering the Secretary of State of State B to produce the encryption key.")*

At this juncture, there is no "Uniform Act" for providing a common means for dealing with issues that are expressed across different states. The Uniform Commercial Code is the most common example of such an Act. There would need to be a similar Act that would cover issues related to states physically holding the data assets of other states.[12]

Conflicts in laws between states, and countries may become a more frequent and relevant issue for cross-jurisdictional collaboratives as cloud computing gains adoption across the states. This intention here is to anticipate and attempt to avoid scenarios where a state government finds itself in the middle of conflicting laws. Cloud providers, including states that begin to offer their services to other jurisdictions, must be aware that once they begin serving residents in multiple jurisdictions, they are subject to data breach notifications and data security requirements for those jurisdictions. *Appendix B presents some examples of statutory assertions – that is, how specific statutes interpret jurisdiction.*

Laws and rules are fixed in time in ways that technology is not. So even the best-intended laws can and increasingly do have unintended consequences later on, often exacerbating the very problem they intended to solve.[13]
Forbes

Recommendations for Mitigating Risks

- Assemble a team for developing and executing on a strategy and delivery process for evaluation, negotiation and ongoing management and governance of cloud computing services. Include the following disciplines: legal, security and privacy, enterprise architecture, data management, records management, project management, subject matter experts from the business side, internal auditing, procurement, and finance.

- Involve legal staff early in planning for and negotiating terms of service. Ensure RFIs and RFPs address potential jurisdictional issues as well as security terms, including validation. Specifying that state law and state courts will be involved in a contract dispute may not be sufficient means for addressing jurisdictional issues involving third parties.

- Ensure you know how to reverse your decisions if it becomes necessary to do so. Identify any costs to exit, including capital costs if you need to return to self-provision of cloud services. Ensure service provider terms of service include provisions for retrieving state government data and deleting state government data held by the service provider. For example: in case of state government changing vendors; the vendor going out of business; purchase of the vendor by another company (particularly a foreign owned company); or service provider non-performance.

- Ensure that the state retains and maintains ownership of data, applications, and business rules. Be exceptionally cautious of granting the cloud provider any ability (licensed or otherwise) to use data for purposes other than your own purposes.

- In certain cases, some data may not be appropriate for cloud deployment.

- Ensure enterprise security policies are in place to prohibit unauthorized creation of cloud accounts. Employees should sign an acknowledgement that they have read and are in compliance with such policy.

- Ensure the cloud provider is providing the appropriate level of security for the classification of information and data that they are entrusted with. Effective operating discipline for security and privacy will reduce the probability of the loss of data which will reduce the probability of litigation which reduces the probability of conflicts of laws.

- Ensure that third party service providers' perform to the same level of performance that has been negotiated with the primary service provider. This may affect the primary service provider's ability to support or respond to elastic demand. The primary service provider should be required to vet third party providers in advance.

- Build awareness of the necessity of proper review of cloud services. Employees should not be creating cloud accounts without that review.

- Ensure state government data is within the geographic limits of the United States. Negotiate to keep data within your state. Until the issue of *physical location* versus *legal location* is resolved, it would be best to avoid conflicts of state laws issues by keeping state data within state borders.

- Recall that special requirements may apply for protection of personally identifiable information (PII).

- Evaluate potential conflict of laws issues related to the cloud deployment options under consideration.

- Explore and evaluate the creation of multi-jurisdictional collaboratives to design and develop cloud solutions and business operations that will be employed by multiple agencies, and jurisdictions. Participate in NASCIO State and Local Collaboration initiative.

- Understand what laws and regulations apply to any inter-enterprise agreements for sharing resources with other governments and/or the private sector.

- Terms of service are important. They should be carefully analyzed and not chosen on simply a "click through" basis. As a state official, the state CIO may have statutory or regulatory responsibilities that cannot be passed through to a private sector vendor.

- Evaluate current state telecommunications contracts for terms and conditions related to hosted solutions. These contracts can provide some valuable elements for cloud contracts.

- Partner with cloud providers to develop a long term *learning* relationship. This relationship must be based on trust.

Appendix A - What Constitutes Personal Data, or Personally Identifiable Information (PII)?

States differ in what they consider personal data. This is a partial list of what is considered personally identifiable information for purposes of determining jurisdictional authority of the state. Loss of this type of data constitutes a data breach which can in turn trigger litigation and potentially involve conflicts of laws in cross-jurisdictional situations.

- first name
- first initial
- last name

  ...in combination with any one or more of the following data elements:

  - Social Security number
  - driver's license
  - state ID number
  - account number
  - credit card number
  - debit card number

    ...in combination with any required security code, access code, or password that would permit access to an individual's

    - financial account

Some states also define the following as personally identifiable information.

- medical information
- health insurance information
- laboratory results
- passport number
- account passwords
- personal ID numbers
- access codes
- unique biometric data
- DNA profile
- electronic registration
- voter registration number
- Individual Taxpayer ID number
- tribal identification
- date of birth
- mother's maiden name
- employee identification number
- digitized or electronic signature

• ***Can PII be Derived? Absolutely!***

Two years ago, the Office of Management and Budget (OMB) created yet another definition of PII. These definitions tend to be very broad. But which definition is referenced in a court? It depends. If a data breach occurs in State A, State A's definition of PII comes into context. There are multiple renditions of state laws regarding PII. California created a definition a decade ago. Many states followed that definition, and then added variations. Over the past two congressional sessions, there have been a series of bills in both houses of the US Congress to distill these definitions. So far, legal definition is pending at the Federal level. The OMB definitions of PII are not statutory. At the federal level, definitions for PII are either in pronouncements or in regulations. These definitions for PII are much more current and take into account a very diverse set of data from multiple sources.

> The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[14]

It is the combination of data that is used to create an identity.

NIST goes further and defines PII as:[15]

> . . .any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. Examples of PII include, but are not limited to:
>
> - Name, such as full name, maiden name, mother's maiden name, or alias
> - Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
> - Address information, such as street address or email address
> - Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
> - Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Given the diverse information contained in various databases, it is possible for an individual to be identified from a broader set of information than has been previously understood. Anymore, it is important to understand what secondary

information can essentially provide the necessary facts to identify an individual. In fact, *aggregation* of relatively *benign* data *can* resolve to an identity. Attributes like voice patterns, facial recognition, signatures (including rate and pressure), purchase patterns, web surfing patterns– all of these things become essentially PII because an identity can be uncovered, discovered, derived, or assembled from this "secondary" data.

The challenge is how to legislate the recognition and inclusion of this data under existing and future statutes and regulations. This *problem* is developing faster than society can deal with it through legislation.

Officials in some states have stated that they knew there were shortcomings in the definition of PII because they don't take account of *aggregation*. However, to update a state's definition of PII using the definitions put forth by the National Institute of Science and Technology (NIST) or OMB, would surface consequences that are difficult to anticipate. For example, statutory use of OMB's definition of PII, would implicate university research information. Researchers have done their best at creating anonymity or "anonymizing" data sets so the state does have a statute that affects education and business that is much broader than what was actually anticipated at the time the legislation was passed. The impact of changing these definitions is not known.

There is indeed a nexus of jurisdictional, security, and data management issues.

It can be anticipated that in court, after a supplier lost secondary data, there will be argument that such secondary data actually constitutes PII. However, this is such a new area of law and given that there haven't been court cases to cite, there is no precedence. As presented earlier in this report, state statutes use the term "reasonable" to describe appropriate security measures. State governments follow the definitions in state statutes and, in accordance with data breach notification, use these basic definitions of PII to determine if notification is necessary.

Another reason that litigation is lagging technological innovation is that in order to get into court, one must allege some *causality*. For example, "*some named party* compromised my identity and fraud has been perpetrated against me." In order to succeed in court, the plaintiff must allege *and prove* the action of the supplier was responsible for the harm suffered. That is very difficult to do at this time. Proximate cause must also be provided. For example, *someone* used citizen's identity and accumulated credit card bills. This is difficult to allege, and difficult to prove causality on the part of the cloud or service provider. The loss of PII may have happened from a waitress that scanned the citizen's credit card, or may be due to a large data breach. In court, the plaintiff *must demonstrate* actions of the individual or company were the *proximate cause* of their loss. This is very hard to do. It requires sophisticated forensics to establish both causality and proximate cause. This is also one of the reasons there is not a lot of related litigation – possibly not any at this point in time.

Appendix B – Statutory Assertions of Select Laws

Examples of Statutory Assertions[16]

Statute	Assertion	Basis
Children's Online Privacy Protection Act ("COPPA") 15 U.S.C. § 6501(2)	Assert US jurisdiction when: 1) US citizens are targeted for harm 2) through computing services used in interstate or international commerce	Location of resident
Gramm-Leach-Bliley Act ("GLBA")	Assert US jurisdiction when: 1) US citizens are targeted for harm 2) through computing services used in interstate or international commerce	Location of resident
Computer Fraud and Abuse Act ("CFAA")	Assert US jurisdiction when: 1) US citizens are targeted for harm 2) through computing services used in interstate or international commerce	Location of resident
Health Insurance Portability and Accountability Act ("HIPAA")	Asserts US jurisdiction • US citizen is harmed	Location of patient / consumer Location of business entity – not the location of the data breach
HITECH Act	Modifies HIPAA and adds penalties. Newer and more prescriptive than HIPAA.	

Statute	Assertion	Basis
USA Patriot Act	Allows law enforcement authorities to access personal information hosted by third parties.	In case of terrorism or severe crime, or to protect national security.
EU Directive - Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data, 1995 O.J. (L 281) 31 Sometimes referred to as the "Privacy Directive" or "The Directive"	Prohibits transferring personal information to countries lacking the same level of protection for EU residents. This includes the U.S.	The Directive required member countries to establish Data Protection Authorities, or "DPAs." These DPAs are put in place to promulgate and administer tough data protection laws. Notably, Spain has been described as the toughest EU data enforcement state.[17]
Cloud Computing Act of 2011	Proposed legislation intended to achieve consistencies internationally regarding privacy, and security, and create law enforcement tools for investigation and prosecution of violators of such laws. Sponsor: Senator Amy Klobuchar (D-Minn.)[18]	To be determined
Alaska stat. § 45.48.010	Asserts jurisdiction over any company that stores personal information of an Alaskan resident.	Location of resident. Physical location of data is irrelevant.
Ariz. Rev. state. § 44-7501	Asserts jurisdiction over any company that does business in Arizona.	Location of resident. Physical location of data is irrelevant.

Statute	Assertion	Basis
Cal. Civ. Code. § 1798.82	Asserts jurisdiction over any entity "doing business" in California. *There is likely not a statutory definition of "doing business". Definition of "doing business" is defined in the courts. Further, courts in different states may define that term differently which creates another level of complexity.*	Location of resident. Physical location of data is irrelevant.
Idaho Code § 28-51-104	Asserts jurisdiction over any entity that owns or licenses personal data of an Iowa resident.	Location of resident.
K.S.A. 17-7307(c)	Provides a basis for general jurisdiction over foreign corporations.[19]	Location of resident.
NV Rev. Stat. (NRS) 603A.215 Security measures, use of encryption, liability for damages.	Asserts jurisdiction over any data collector (both public and private sectors) doing business in Nevada.	Location of resident. Physical location of data is irrelevant.

Appendix C – Jurisdictional and Legal References

The Association of American Law Schools (AALS)
www.aals.org/
AALS is a resource for the improvement of the quality of legal education by networking law school faculty, professional staff and deans to information and resources. AALS is the principal representative of legal education to the federal government, other national higher education organizations, learned societies and international law schools.

The Association of American Law Schools Section on Conflict of Laws has requested an annual survey of "choice of laws" for over twenty years. The survey provides details on cases, the courts in which such cases were heard, and the rationale for selecting the law of one jurisdiction over another. The Survey covers cases decided by American state and federal appellate courts.

One source for these surveys is the Social Science Research Network at ***www.ssrn.com***.

- **Choice of Law in the American Courts in 2010: Twenty-Fourth Annual Survey**
  http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1737558

The American Society of Comparative Law
The American Society of Comparative Law, Inc. (ASCL) is the leading organization in the United States promoting the comparative study of law. Founded in 1951, it is a thriving organization of more than 100 institutional sponsor members, both in the United States and abroad, and a growing number of individual members. It is a member in good standing of the American Council of Learned Societies and International Association of Legal Science. The Society publishes The American Journal of Comparative Law, the outstanding American publication of scholarship on comparative law. It holds annual meetings at which comparative law scholars present research and critically examine important legal issues from a comparative perspective. In addition, it provides support to other scholarly conferences both in the Unites States and internationally that deal with comparative law.

The American Society of Comparative Law is associated with the International Academy of Comparative Law and participates in the Academy's quadrennial Congresses bringing together experts in comparative law from around the world. The Eighteenth Congress was held in Washington, DC in 2010 and the society played a key leadership role in its organization. Furthermore, the Society often cooperates with it counterparts in other countries
www.comparativelaw.org

Bureau of National Affairs
www.bna.com.
"Privacy and Security Law – Contracting for Cloud Computing Service: Privacy and Data Security Considerations," by Tanya L. Forsheit, ISSN 1538-3423. Bureau of National Affairs, www.bna.com.

Cyberspace Lawyer - articles
Mrazik, R., Reingold, B., "Cloud Computing: The Intersection of Massive Scalability, Data Security and Privacy – Part I," *Cyberspace Lawyer*, (June 2009). Retrieved on November 15, 2011, from www.perkinscoie.com/files/upload/ps_09-06_cloud_computing_article.pdf.

Reingold, B., Mrazik, R., "Cloud Computing: Industry and Government Developments – Part II," *Cyberspace Lawyer*, (September 2009). Retrieved on November 15, 2011, from www.perkinscoie.com/files/upload/P&S_09-09_Westlaw_Document_13_43_53.pdf.

Reingold, B., Mrazik, R., D'Jaen, M., "Cloud Computing: Whose Law Governs the Cloud? – Part III," *Cyberspace Lawyer*, (January-February, 2010). Retrieved on November 15, 2011 from www.perkinscoie.com/files/upload/SEA_10-03_Westlaw_Document_09_48_34.pdf.

Cloud Computing Law Journal
www.cloudcomputinglawjournal.com/

The Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510-2522)

Appendix D – Cloud References

The Australian Government Cloud Computing Strategic Direction Paper
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 Computing Strategic Direction paper to explore the opportunities and impacts of cloud computing.

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
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 The SCA governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers ("ISPs"), telephone companies, and cell phone service providers.

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
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 Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Federal Cloud Computing Strategy
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)
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 500s & entrepreneurial user companies, major security vendors, government, & academics. Working together, members drive approaches and standards for a secure, collaborative online business world.

National Institute of Standards and Technology Cloud Computing Program
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
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.

Appendix E – Data Management References

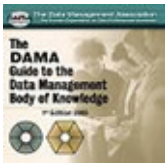
NASCIO on Data Governance – *www.nascio.org/publications*

Data Governance - Managing Information As An Enterprise Asset: Part I - An Introduction
April 2008
Data governance entails a universe of concepts, principles, and tools intended to enable appropriate management and use of the state's investment in information. Part I on data governance presents an introduction that describes the basic concepts. Governance, and particularly data governance, is an evolutionary process. It begins with an understanding of the current investment and then manages that investment toward greater value for the state.

Data Governance Part II: Maturity Models – A Path to Progress
March 2009
Data governance maturity models provide a foundational reference for understanding data governance and for understanding the journey that must be anticipated and planned for achieving effective governance of data, information and knowledge assets. This report continues to build on the concepts presented in Data Governance Part I. It presents a portfolio of data governance maturity models.

Data Governance Part III: Frameworks – Structure for Organizing Complexity
May 2009
This issue brief presents the concept of frameworks that describes what constitutes a data governance program, with a focus on frameworks from the Data Management Association (DAMA), the Data Governance Institute (DGI), and IBM. Use of frameworks can assist state government in planning and executing on an effective data governance initiative. They assist in achieving completeness in a program. In any subject or discipline frameworks and maturity models assist in describing the scope – both breadth and depth – of an initiative. This holds true as well for data, information and knowledge.

DAMA Data Management Body of Knowledge – DMBOK



DAMA International is a non-profit, vendor-independent, global association of technical and business professionals dedicated to advancing the concepts and practices of information and data management.
www.dama.org/i4a/pages/index.cfm?pageid=1

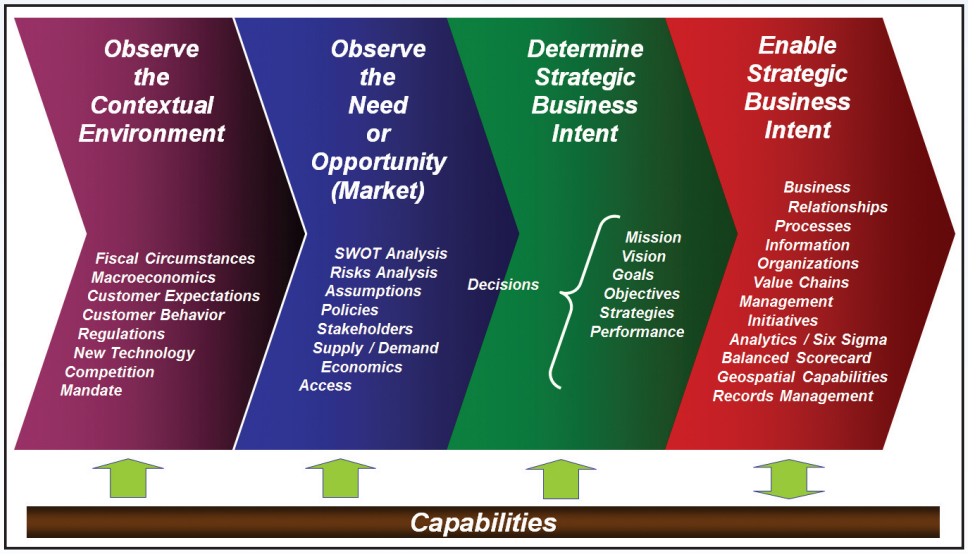
The Data Administration Newsletter

Welcome to TDAN.com, the industry leading publication for people interested in learning about data administration and data management disciplines & best practices. Each monthly issue addresses the most challenging issues of the day.

Appendix F – NASCIO Enterprise Architecture – Definition and EA Value Chain

Enterprise Architecture is a management engineering discipline that presents a holistic, comprehensive view of the enterprise including strategic planning, organization, relationships, business process, information, and operations.

The organization must be viewed as a fluid – changing over time as necessary based on the environment and management's response to that environment.



Contributors

Rick Becker, Legal Counsel, Office of the CIO, State of Nebraska

Patricia Cummens, Account Executive, ESRI Corporation

Stu Davis, Chief Information Officer and Assistant Director, Ohio Department of Administrative Services, Office of Information Technology

Brenda Decker, Chief Information Officer, State of Nebraska

Paul Warren Douglas, Enterprise Architect, State of Washington

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

James Earl, J.D., Executive Director, Technological Crime Advisory Board, State of Nevada

Lauren Farese, Public Sector Senior Director, Oracle Corporation

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

James Ferreira, Chief Information Officer, Office of the New Mexico Attorney General

Jeremy Foreman, *Public Sector Enterprise Architecture Program Director, Oracle*

Di Graski, *Principal Court Management Consultant, National Center for State Courts*

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

Sam Holcman, President of the Zachman Institute for Framework Advancement (ZIFA), the Chairman of the Pinnacle Business Group, Inc., and the Managing Director of the Enterprise Architecture Center of Excellence (EACOE)

Christopher G. Ipsen, CISSP-ISSAP, CISM, Chief Information Security Officer, State of Nevada, Department of Information Technology

Bert Jarreau, Chief Information Officer, National Association of Counties (NACO)

Hedda Litwin, J.D., Cyberspace Law Chief Counsel, National Association of Attorneys General

Dr. Dave McClure, Associate Admin for Citizen Services and Innovative Technology (OCSIT), Government Services Administration Office of Citizen Services and Innovative Technologies

Bob McDonough, *Chief Cloud Architect, State of Michigan*

Darlene Meskell, Director, Global Government Innovation Networks, Government Services Administration Office of Citizen Services and Innovative Technologies

Maury Mitchell, Director State of Alabama Criminal Justice Information Center

Michael Muilenburg, Data Practices Compliance Official, Office of Enterprise Technology, State of Minnesota

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

Daniel J. Paolini, CBIP, CDMP, CDPS, Deputy Chief Technology Officer, Data Management, Information Architecture and Administrative Services Affinity Group, State of New Jersey Office of Information Technology

Carolyn Parnell, Chief Information Officer, State of Minnesota

Doug Robinson, Executive Director, NASCIO

Charles Robb, *Senior Policy Analyst, NASCIO*

Bill Roth, Chief Information Technology Architect, State of Kansas

David Taylor, Chief Information Officer, State of Florida

Glenn J. Thomas, PMP, CDMP, CPM, Director, IT Governance, Commonwealth of Kentucky, Office of Technology

Shawn K. Vaughn, Membership & Communications Coordinator, NASCIO

Joseph Vitale, Executive Director, National Association of State Workforce Agencies (NASWA)/Information Technology Support Center

Tom Walters, Enterprise Business Architect, Commonwealth of Kentucky, Office of Technology, Office of Enterprise Technology, Division of IT Governance

[1] *A New C⁴ Agenda – Perspectives and Trends from State Government IT Leaders.* October 2011. NASCIO, TechAmerica, and Grant Thornton. Available at www.nascio.org/publications/.
[2] Ristenpart, T., Tromer, E., Shacham, H., Savage, S., "Hey, You, Get Off of My Cloud: Exploring Information Leakage I Third-Party Compute Clouds," Retrieved on October 28, 2011, from http://cs.tau.ac.il/~tromer/papers/cloudsec.pdf.
[3] NASCIO definition of enterprise architecture and the NASCIO Enterprise Architecture Value Chain are presented in *Appendix F* and also a number of NASCIO publications available at www.nascio.org/publications. These include: *Do You Think? Or Do You Know? Part II – The EA Value Chain, The Strategic Intent Domain, and Principles; Transforming Government through Change Management: The Role of the State CIO.*
[4] Burke T. Ward & Janice C. Sipior (2010): The Internet Jurisdiction Risk of Cloud Computing, Information Systems Management, 27:4, 334-339
[5] *A New C⁴ Agenda, Perspectives and Trends from State Government IT Leaders*, October 2011. Published jointly by NASCIO, TechAmerica and GrantThornton. P. 19. Retrieved on October 28, 2011, from www.nascio.org/publications.
[6] Note, the Association of American Law Schools requests an annual survey covers cases decided by American state and federal appellate courts. See https://memberaccess.aals.org/eweb/dynamicpage.aspx?webcode=ChpDetail&chp_cst_key=6f59fb1f-b1a1-488a-bd97-2f39ad524d09
[7] Forsheit, T.L., *Contracting for Cloud Computing Service: Privacy and Data Security Considerations*, Privacy & Security Law Report, 9PVLR20, 05/17/2010. The Bureau of National Affairs, Inc. http://www.bna.com.
[8] Reingold, B., Mrazik, R., *Cloud Computing: Industry and Government Developments (Part II).*, Cyberspace Lawyer, September, 2009. 14, No. 8. P. 3. Retreived on August 17, 2011, from http://www.perkinscoie.com/files/upload/P&S_09-09_Westlaw_Document_13_43_53.pdf.
[9] Wernick, A.S., "Warning Cloud." 2010. Retrieved on October 28, 2011, from http://www.wernick.com/publications.html.
[10] Reingold, B., Mrazik, R., *Cloud Computing: Industry and Government Developments (Part II)*, Cyberspace Lawyer, September, 2009. 14, No. 8. P.2. Retreived on August 17, 2011, from http://www.perkinscoie.com/files/upload/P&S_09-09_Westlaw_Document_13_43_53.pdf.
[11] Gartner Group, Privacy in the Cloud, Published: February 25, 2011, Analyst(s): Carsten Casper, G00210881
[12] Interview with Mr. James Earl, J.D., State of Nevada, Executive Director, Technological Crime Advisory Board. NASCIO Conference Call with states of Michigan, Delaware and Nevada on March 4, 2011.
[13] Downs, L., *The Law of Disruption Occupies Wall Street*, Forbes. Retrieved on October 18, 2011, from http://www.forbes.com/sites/larrydownes/2011/10/16/the-law-of-disruption-occupies-wall-street/5/.
[14] Definition of PII as presented on the website for the Department of Commerce Chief Information Officer – and cited by the Office of Management and Budget, OMB Memorandum M-07-16. Retreived on October 31, 2011, from http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/DEV01_002682#P126_15356.
[15] *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122. April, 2010. pp. E-1 to E-2. Retrieved on September 6, 2011, from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

[16] Reingold., B., Mrazik, R., D'Jaen, M., *Cloud Computing: Whose Law Governs The Cloud? (Part III)*, Cyberspace Lawyer, January-February, 2010. 15, No. 1. Retreived on August 17, 2011, from http://www.perkinscoie.com/files/upload/SEA_10-03_Westlaw_Document_09_48_34.pdf.

[17] EU Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data, 1995 O.J. (L 281) 31.

[18] *Evaluating the Cloud Computing Act of 2011*, Brookings Institute Forum, June 16, 2011. Retrieved on August 19, 2011 from http://www.brookings.edu/events/2011/0616_cloud_computing.aspx

[19] See further detailed analysis, Supreme Court of the State of Kansas, Docket No. 91,702. Retrieved on November 15, 2011, from www.kscourts.org/cases-and-opinions/opinions/supct/2006/20061109/91702.htm.

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.