

Arkansas Enterprise Cloud Strategy

Vision

Leverage the benefits of the cloud while ensuring the proper levels of security to protect state assets

Arkansas Goals:

Strengthen education, enhance economic development, improve operational efficiency, increase citizen access, provide public safety, and safeguard the environment.



- Explosive growth in cloud services
- Increased access to broadband is a catalyst for increased cloud services
- Mobile devices will continue to improve and usage expands. The cloud enables access to any document from any location using a variety of devices in many form factors
- Consumerization of information technology and the convergence of mobile, cloud, social media and information
- Cloud Service Management to harmonize the different cloud applications needed
- Service Level Agreements are written into contracts
- Cloud Security expands to encompass privacy, compliance, and governance
- More cloud options – anything as a service
- Likely mergers, acquisitions and consolidation will impact service providers
- Cloud solutions require access to the Internet which increases network usage and can cause bottlenecks
- Software-defined networking (SDN) will become more pervasive and increase the utilization of available network resources
- Business cloud backup is effecting employment. Backup jobs previously carried out by several workers can now be automated over networks to cloud service providers



Cloud computing is the use of scalable and elastic computing resources (hardware and software) that are delivered as a shared service using Internet technologies and is a pay-per-use subscription model. Cloud computing is not defined by one product or technology. It is a style of computing that characterizes a model in which providers deliver IT-enabled capabilities to consumers.

Cloud Types:

Public Cloud - This is a service whereby a third party, such as Amazon or Microsoft, provides computing capacity, data storage, etc., on a variable-cost basis—with the customer paying the supplier on a per unit basis – scalable, elastic, self-provisioning. Open access, fully shared

Private Cloud - Consists of on-premise computing or data storage resources available automatically. Closed access

Hybrid Cloud – Variations of both that limit access and limit sharing depending on requirements

Cloud Brokerages – A relatively new service that addresses the needs of business where they need multiple cloud services potentially from multiple cloud providers. Organizations today are combining cloud services from multiple providers (such as Google, Amazon, Salesforce) and customizing the solutions to support their unique business processes

Personal Clouds – The forces of consumerization (social, mobile and cloud) have led to services where individuals store content and access personal, business and government services (store content like voter registration, tax info, etc.). Ease of synchronization across multiple devices and screens (mobility). Content and applications are accessible to users via whatever device they are using and whatever their location. Dropbox is the best-known cloud storage and sync provider with a cross-platform offering. The personal cloud along with bring your own device initiatives will help increase productivity as users synchronize using cloud-based services, enabling use of professional and personal applications.

SaaS – Software as a Service Customer relationship management, enterprise content management, office suites, project and portfolio management, web conferencing, social software suites

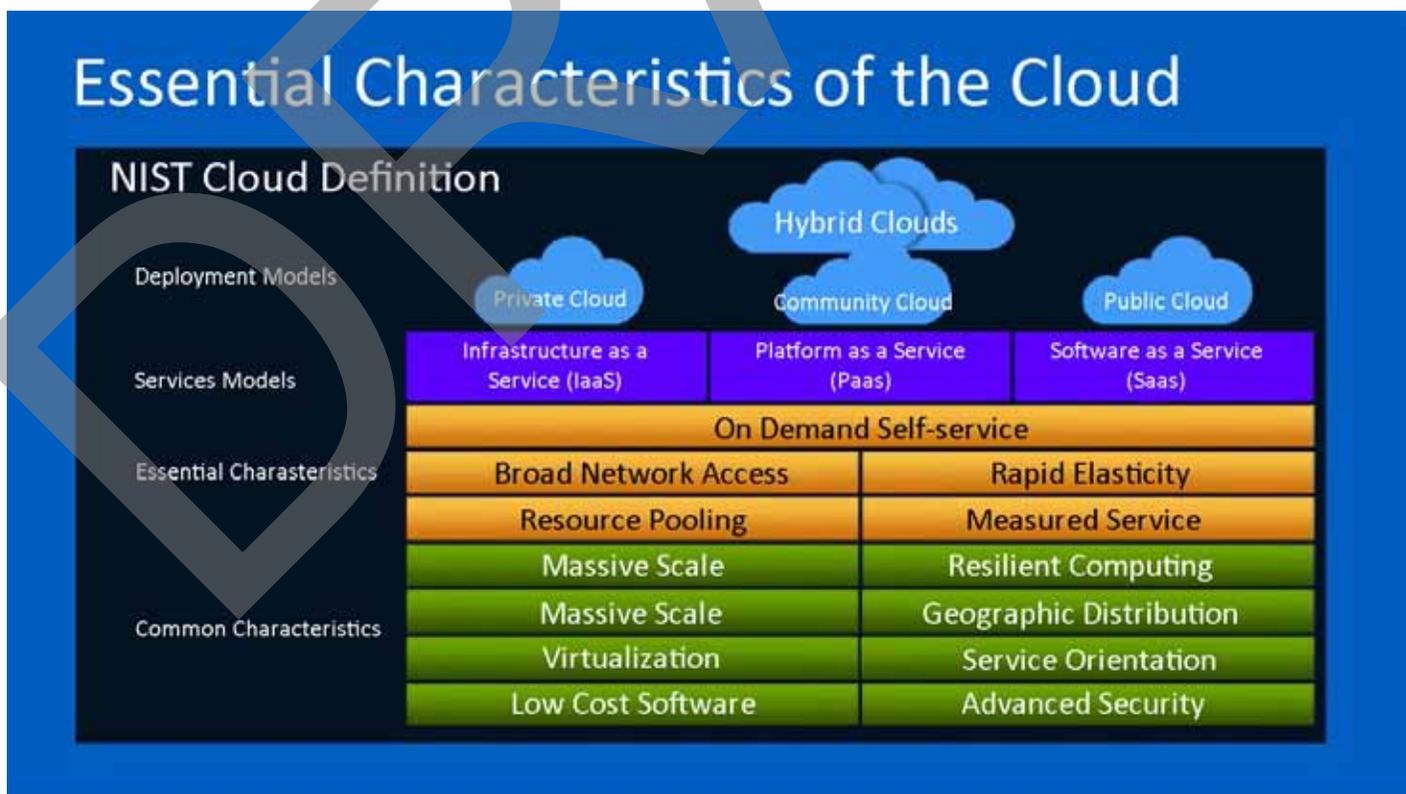
PaaS – Platform as a Service Application development, application infrastructure and middleware, database management systems, business intelligence platforms

IaaS – Infrastructure as a Service Compute, storage, print

Cloud Computing Service Layers

Cloud Computing Services	Description
System Infrastructure	Virtualized system software on which users can run any application
Application Infrastructure	A set of services that parallels traditional middleware and development technologies
Applications	Designed for global-class delivery, delivered as a service via Web-centric architectures to a browser
Information	Content access and search services or data services
Business Processes	Any business process delivered as a service via the Internet
Management and Security	Services to manage the access, use, delivery and service levels of cloud services

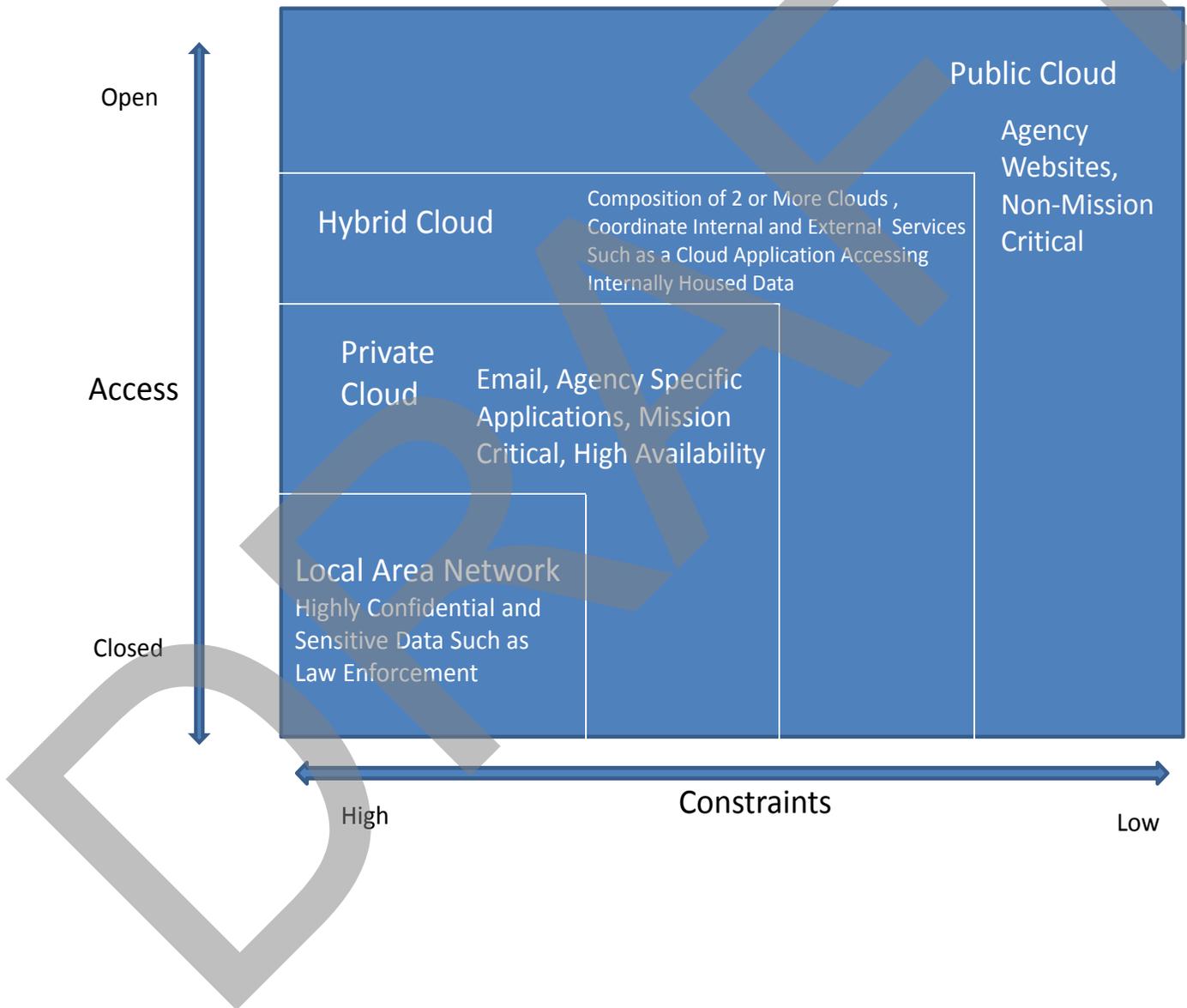
The National Institute of Science and Technology (NIST) has produced many reports on computer systems technology including cloud. The following graphic is NIST's illustration of essential elements in a cloud solution.



The ARCloud Landscape

Agency business functions have differing information technology requirements related to availability, security and cost. The following graphic depicts an overall landscape for the types of business functions and their suitability for cloud services.

ARCloud Landscape



Available Services in the Private ARCloud

Infrastructure as a Service (IaaS):

Arkansas Department of Information Systems (DIS) has equipment used to support operations, including storage, hardware, print, servers and networking components. DIS owns the equipment and is responsible for housing, running and maintaining it. You pay for what you use. The state of Arkansas offers the following IaaS services:

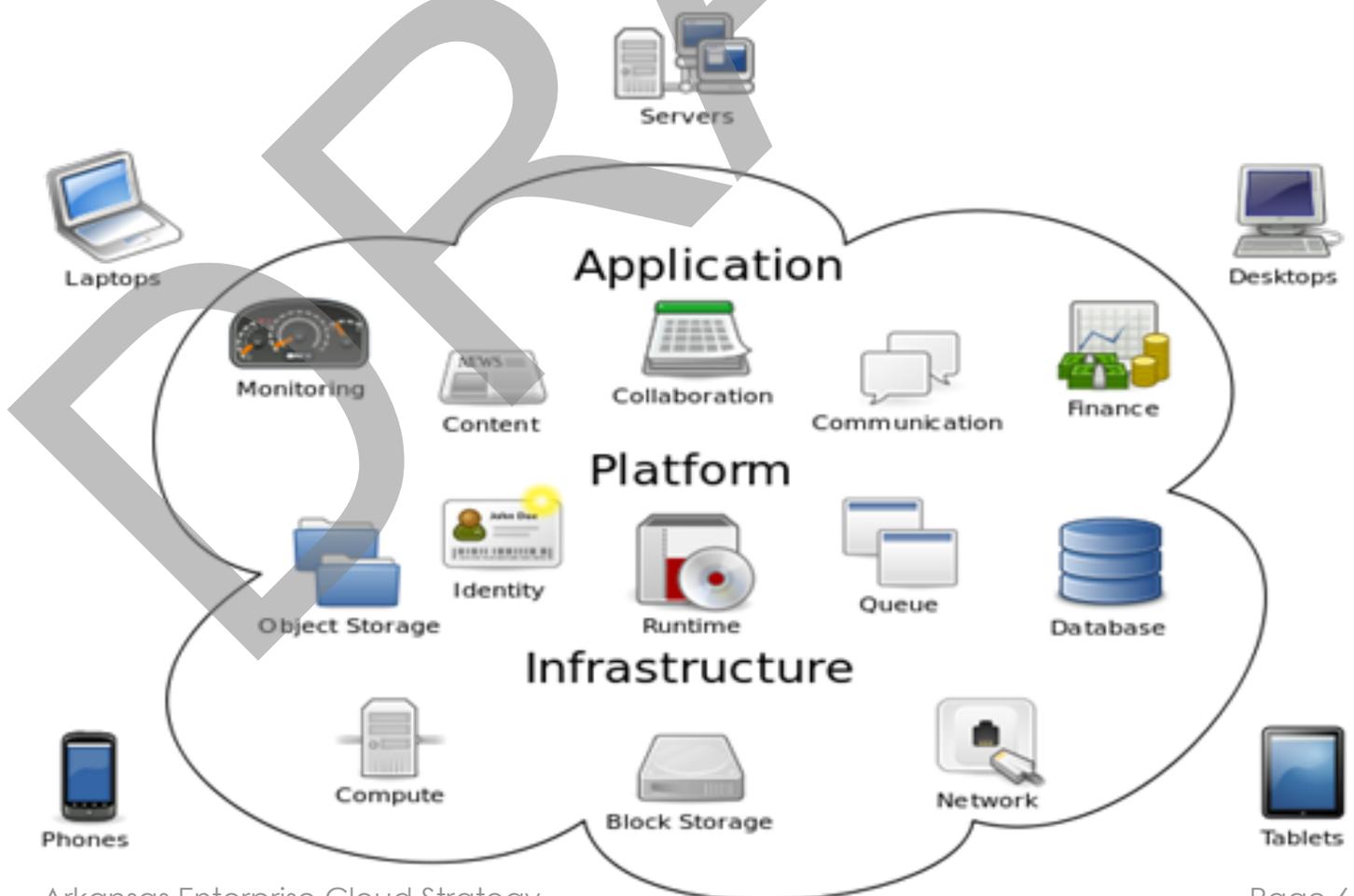
- Managed Windows Virtual Machine Hosting
- Unmanaged Windows Virtual Machine Hosting
- Managed Linux Virtual Machine Hosting – Open Source
- Unmanaged Linux Virtual Machine Hosting – Open Source
- Managed Linux Virtual Machine Hosting - Proprietary
- Unmanaged Linux Virtual Machine Hosting – Proprietary
- Enterprise Disk Storage Services
- Enterprise Tape and Backup Storage Services

Platform as a Service (PaaS):

Providing a computing platform and a solution stack as a service. This includes the storage, hardware, servers, networking and software stacks needed to provide the solution.

The state of Arkansas offers the following PaaS services:

- Shared Microsoft SQL Server Hosting
- Shared IBM DB2 Hosting
- Shared Microsoft Exchange Email Hosting
- Shared Microsoft Sharepoint Hosting



Benefit	Description
Cost Reduction	<p>By utilizing a subscription or pay as you go model the costs are shifted from capital expense to operational expenses with minimal upfront costs. Savings can be realized in the following areas:</p> <ul style="list-style-type: none"> • Labor reduction • Software licensing • Technical and user support • Maintenance and system upgrades • Infrastructure (servers, power, cooling, floor space)
Enhanced Productivity	User mobility and universal access can increase productivity
Optimized Resource Utilization	Existing resources can be re-tasked
Access to Enterprise Tools	The ability to access enterprise class software and infrastructure that may have been unaffordable without a service pay as you go model
Scalability	The ability to expand or contract as needed
Increased Agility	The ability to more quickly provision a service or improve the speed of deployment
Increased Reliability	Cloud service providers typically have redundant sites to support services in the event that an incident disrupts service at any one location
Risk Transfer	Risk can be transferred to the cloud service provider
Increased Business Opportunities and Innovation	Allows addition or expansion of services into areas where services were unavailable or without optimum solutions in place
Trial Periods	Ability to consume or try a service before investment decisions are made
Risk	Description
Security	<ul style="list-style-type: none"> • E-discover and FOI • Data loss prevention • Encryption
Legal and Contractual	Ensure the state controls data ownership
Financial	Cost of the cloud service over time needs to be known as well as the cost of not using cloud service.
Performance	Cloud provider alone does not ensure performance. The bandwidth available to the user is a critical component of performance.
Integration	Cost and difficulty of integration of cloud services with other required state services must be determined
Governance	Organizations must ensure that the cloud provider is protecting data and performing according to the contract and related service level agreement



One of the most difficult tasks in deciding whether or not a cloud solution is the right decision is quantifying the total costs and expected benefits. Costs include direct and indirect costs. Costs should also be anticipated over the life of the project, short, medium, long and retirement. Benefits include tangible and intangible. Return on investment or ROI is one financial metric that can be used to justify business investment.

$$\text{ROI} = (\text{Gain From Investment} - \text{Cost of Investment}) / \text{Cost of Investment}^*$$

If the result from the ROI equation is greater than zero, it means the return is greater than the cost and can be considered a beneficial investment. Cloud computing costs and benefits are not always readily known and it is advisable to use a business case supported by multiple financial metrics.

To properly evaluate the costs and benefits of cloud computing, enterprises need to:

- Clearly document expected benefits in terms of rapid resource provisioning, scalability, capacity, continuity and the cost reductions that the cloud services offer.
- Define the true life-cycle cost of IT services provided internally or through a cloud service provider.
- Balance cost with functionality, resilience, resource utilization and business value.
- Look beyond cost savings by considering the full benefits of what cloud services and support can provide.
- Periodically evaluate performance against expectations.

*ISACA

If there is a determination that a sufficient business case supports cloud computing services, then there is a lengthy list of topics to address in any contract providing these services. These basic topics relate to the assignment and assumption of risk between the contracting parties, and the risks may change based on several factors: 1) the information, applications, or data that will be placed in the cloud, 2) the result if the information is compromised, and 3) the level and cost of acceptable mitigation.

The following topics, while not an exhaustive list, demonstrate some of the complexities to be addressed in any agreement between a customer and the vendor of cloud computing services:

- Data security
- Management of data breach or security incidents
- Access to network traffic
- Arbitration
- Indemnification
- Advertising



- Reliance upon or reference to external agreements
- Affiliates
- Geographic status/ data sovereignty
- Third-party security audits and access to data
- Statutory compliance
- Termination and transition/migration of data
- Media/data destruction and certification
- Vendor bankruptcy, sale, or merger
- Applicability or effect of contract between integrator and cloud provider
- Disaster Recovery plan for vendor and integrator
- Asset availability and physical location
- Hardware/software compatibility between parties
- Outages and down time – scheduling and reduction in cost
- Maintenance - notice, upgrades, patches, and version control
- Additional costs for information access – Freedom of Information Act, litigation, e-discovery, litigation hold, subpoenas
- Intellectual Property
- System integrity – boundaries and duties between parties
- Data, back-up, and network traffic encryption
- Employee screening and background checks
- Non-disclosure agreements
- Use of agency tools or security applications in cloud services
- Legal proceedings and costs of litigation
- Separation of classified and unclassified information
- Service levels for provision of cloud services

In addition, the application of Arkansas law and statutory provisions is another overlay of legal requirements that applies to any public-sector contract. Given the range and depth of topics to be addressed in any cloud services contract, trained legal review cannot be over-emphasized or over-looked in the drafting or negotiation process.

Cloud computing presents security considerations that must be addressed before state data and business processes are placed in the cloud. The classification of the state data in terms of criticality and sensitivity must also be taken into consideration. For example, is it appropriate to put law enforcement records into the cloud for use by law enforcement officials? Is it appropriate to have an informational web site hosted by a cloud provider?

Additionally, security mechanisms protecting state data must be defined and assigned to the appropriate entity. For example, data hosted in the cloud and transported to the cloud may be encrypted by the agency, but conducting background checks on the cloud provider employees would be the responsibility of the provider. Securing state data is the shared responsibility of both the state entity and the cloud providers.

Most data classified as being sensitive is associated with a law or mandate requiring specific security measures. Some of the measures will likely be controlled by the cloud provider, such

as server patching. The cloud provider will need to verify that security mechanisms are in place either by an in person audit or proof of a third party audit. In a situation where the data is hosted by the agency or at the Department of Information Systems, auditors verify security measures are in place in person. In a cloud situation, the data may be spread across multiple data centers and across multiple states or even countries. Cloud providers must be able to prove compliance with security mandates.

A cloud provider can submit to a third party for a security assessment to prove adequate security is in place. Providers can also attest to being certified as meeting known security mandates such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry standard (PCI), the Family Educational Rights and Privacy Act (FERPA) and the federal standards created by the National Institute of Standards and Technology (NIST). Since the state's data may be housed at multiple cloud provider locations, it is impractical for the state entity to audit for appropriate security mechanisms. Cloud providers will likely be reluctant to do so due to the fact that the provider is protecting data belonging to other customers at the same location.

Applications accessing state data in the cloud must also process and transmit the data in a secure manner. As in the case of a data hosting solution, applications offered by cloud providers should be evaluated to ensure security mechanisms are in place to protect sensitive state data. Data transmissions between the cloud provider and state employee should be encrypted to avoid data interception. Cloud providers need to describe the security mechanisms in place within the applications themselves and, if possible, attest that the applications have undergone security testing to discover vulnerabilities. Ask if the applications were developed with robust software development lifecycle (SDLC) practices. In other words, were the applications written with security in mind to prevent unintended or unauthorized actions by the application.

No matter what the sensitivity level of state data hosted in the cloud, cloud providers should take appropriate steps to ensure their employees are vetted by background checks. Cloud providers also need to demonstrate that appropriate access control mechanisms are in place for their employees. Require the cloud provider to describe the security provisions in place to protect your data from being accessed by their employees. A way to mitigate this risk would be for the agency to encrypt the information housed at the cloud provider facility.

Strong authentication should be in place to ensure that only authorized people have appropriate access to state data. Another way to protect state data would be to employ data loss prevention technologies. Data originally hosted locally in an environment over which your organization had direct control is now comingled with data belonging to other organizations. An agreement must be made with the cloud provider in the event of a data breach to describe the breach investigation approach. The approach must include whether the provider would be willing to allow a physical and logical investigation by law enforcement personnel in the event prosecution is likely. If the provider is aware of the breach, how is the Arkansas entity notified and what is the timeframe for that notification? Does that vendor have the ability and responsibility to retain information relevant to the security investigation in order to comply with the state's requirements? Could the state organization run its own forensic software on the state data in the cloud? In the event of a breach found to be the fault of the provider, will the provider pay for the costs associated with the breach activities,

including the notification process for those impacted by the breach? The vendor must indicate an understanding of the Arkansas Personal Information Protection Act (A.C.A. § 4-110-106 (2012)) in order to identify the conditions that constitute a breach.

Another aspect of cloud security would be the provider's ability to fend off cyber attacks. Is the provider protected from distributed denial of service attacks? Does their company monitor attempts to access the data housed at their facilities, including the unauthorized attempts? Are the attempts to access data at the cloud provider inspected thoroughly?

Availability is an aspect of cyber security. State data should be backed up at another location other than the cloud provider location to minimize risk. If the cloud provider is providing disaster recovery services, learn the specifics of their strategy. Similarly, the provider should specify the schedule for server and software updating and maintenance.

Finally, state entities need to understand and adhere to the data destruction process when state data is no longer hosted by the provider. The method of data destruction must be effective and the fact that the data was destroyed must be documented.

Governance

It is important to continually monitor cloud solutions to ensure it is meeting objectives. Governance ensures the effective and efficient use of cloud services to achieve the goals of the organization. Make sure the goals of the service are agreed upon and verifiable. If possible document performance measures prior to cloud implementation and manage the service to the measures. Performance measures aligned to business objectives help cost containment and risk management. It may be necessary to develop new policies and procedures regarding new activities related to cloud services especially around security, interfaces to other systems and change management.

Latency

Private cloud architecture provides the ability to control both ends of the link. Network latencies are significantly reduced in a private cloud because traversal of the public Internet to the end user is typically not required. The absence of public traffic would result in increased bandwidth thus improving application performance and user response times. Storage performance can also be optimized in a private cloud environment with the use of high performance storage hardware and the configuration of high-bandwidth connectivity to those devices.

User Access

Users must be able to access cloud services over a variety of current and emerging platforms. Users must have appropriate access to these cloud services whether at work or in the field. The increased functionality of mobile devices, tablets and smart phones increase user productivity when out of the office. Cloud services must be readily available and easy to use on mobile devices.

Successful implementation would allow cloud services to dynamically provision and optimize its own construction and resource consumption over time.

Redundancies must be implemented that would allow services to recover from routine and extraordinary events that might cause some or all of its parts to malfunction avoiding service interruption.



Cloud Service Procurement

As organizations consider cloud solutions, the following activities should be undertaken as a part of the evaluation process. Prospective benefits need to be examined carefully and mapped against a number of challenges, including security, lack of transparency, concerns about performance and availability, the potential for vendor lock-in, licensing constraints and integration needs. See **Appendix A: Cloud Computing Services** for additional things to consider before signing a contract.

Activity	Description
Build a Business Case	If, when, where, how and why cloud services should be used. Conduct initial cost benefits analysis and risk identification
Classify Data	Data must be classified according to its confidentiality and sensitivity. Depending on how it is classified determines the level of security necessary to safeguard state data
Define Processes	How do processes align with goals and relationships with other processes
Define any Integration Points with Existing Systems	Identify any integration needs and ensure data is stored in a standardized way. Data linked with other systems increases the value of the information.
Amend IT Plan to Include the Cloud Solution	New projects not already defined in the agencies IT plan must submit an amendment that describes the project
Vendor Evaluation	Examine the providers implementation of elasticity and shared services
Securing, Managing and Governing Cloud Services	Define roles and responsibilities



The state has a responsibility to build a comprehensive strategy that encompasses the following best practices. The following strategies and objectives serve as the state level strategy which will be carried out by the state cloud working group and other stakeholders.

State Cloud Strategies

1: Educate state government agencies on suitable cloud applications

Objective 1: Create a strategy that contains best practices and references on the cloud

2: Identify state government business functions that are candidates for cloud computing

Objective 1: Increase value to the customers or lower cost of service to customers

Objective 2: The ability to access enterprise tools potentially increases customer benefit

Objective 3: Agility and being faster to respond to changing customer demand

3: Build a robust private cloud infrastructure capable of supporting Arkansas state government needs through 2020.

Objective 1: Utilize existing enterprise email services

Objective 2: Utilize existing enterprise storage capacity

Objective 3: Utilize existing enterprise virtualized servers

4: Procure cloud services through a standardized process

Objective 1: Ensure that all cloud solutions are included in state agency IT plan

Strategies should be adopted at the agency and state level to ensure the best use of cloud technologies in Arkansas. Information technology is rapidly changing and cloud service is an evolving method of computing that is rapidly growing in popularity. However, there are many aspects of cloud computing that must be fully understood before adopting cloud services.

If agencies adopt cloud services, their agency information technology plan must include information regarding the project or application.



Agency Cloud Strategies

1: Build a business case for each application being considered for the cloud.

Objective 1: Identify cloud performance metrics to document tangible benefits

Objective 2: Ensure adequate bandwidth exists or is available to accommodate cloud solutions for the present and future

Not all applications are a good fit for clouds. Good candidates are not mission critical and are not tightly integrated with other important applications.

2: Classify data according to sensitivity and confidentiality. One of the biggest hurdles to widespread cloud adoption is organizations inability to classify data.

Objective 1: Prior to uploading any data into a public or hybrid cloud model, ensure that all sensitive or critical data is encrypted or obscured for data at rest, or in motion, to prevent unauthorized disclosure.

3: Ensure potential cloud solutions have a positive financial benefit

Objective 1: Determine tangible and intangible benefits to the cloud solution prior to entering an agreement and ensure those benefits are realized after implementation

Objective 2: Determine the total cost of operations for the cloud solution prior to entering an agreement (upfront costs, recurring costs and termination costs)

Objective 3: Use generally accepted accounting calculations where applicable to determine financial benefits –Return on Investment, Total Cost of Operations, Net Present Value, Internal Rate of Return and payback period

Objective 4: Small to mid-size organizations have been able to more clearly demonstrate benefits than large organizations who already have economies of scale

4: Identify and mitigate risks presented by the cloud service provider

Objective 1: Ensure compatibility with existing or future IT solutions

Objective 2: Establish a Service Level Agreement (SLA) to define guaranteed uptime and ensure performance is not degraded in a multitenant model

Objective 3: Ensure the cloud service provider is compliant with all applicable laws and policies

Objective 4: Ensure that cost controls are in place that are based on usage

Objective 5: Ensure portability of the technology so that the solution can be moved to another service provider or hosted if necessary

Objective 6: Ensure individual business units work with IT to adopt a governance framework

Objective 7: Limit customization of the cloud solution to minimize costs associated with future changes or upgrades

Objective 8: Evaluate staff to ensure they have the skills and competency required to support cloud services and if necessary, plan to develop or acquire the necessary skills.

5: Plan for service interruptions

- Objective 1: Ensure that cloud service provider is capable of providing service from multiple locations to mitigate the risk of an unplanned outage at the main location
- Objective 2: Ensure that the network can rapidly add or reallocate capacity to the disaster recovery-business continuity site or any other alternate location as necessary

6: Plan for service retirement

- Objective 1: Evolving business needs may necessitate cloud service retirement. Ensure that contractual terms exist for how the service is shut down, how the data is provided to the customer and how all remaining data residing within the cloud is removed
- Objective 2: Ensure data is retained for compliance with the Arkansas Records Retention Schedule or for its historical value

Conclusion

As cloud service providers are becoming more mature in their offerings in terms of security and compliance, the potential savings are leading to increased interest and adoption. Governments should evaluate the cost of cloud offerings versus the benefits to get a true picture of the value of the service. Additionally, government should seek opportunities for collaboration with other public sector entities to realize economies of scale and maximize efficiencies. Let this document serve as a guide when evaluating cloud services for your organization.



Appendix A: Cloud Computing Services

CLOUD COMPUTING SERVICES: QUESTIONS TO ASK & THINGS TO TAKE INTO CONSIDERATION BEFORE SIGNING A CONTRACT

Considerations: When you are utilizing cloud computing services, your data, your business operations are being turned over (outsourced) to be managed by a vendor, thus you will no longer have direct control of the data, applications, user access, or hardware configurations. Assume the worst, if that data was destroyed or leaked out to the general public how would it affect/impact your business? Keep in mind that to ensure that the vendor is providing you the right level and quality services that you want that these performance provisions **MUST** be specified in the contract. If the performance level expectations you have are **NOT** specified in the contract then the vendor does **NOT** have to provide that level of service.

Here are some questions to ask and consider in dealing with cloud services vendors:

*Contract Issues:

Infrastructure/Security - All cloud service vendors are **NOT** created equally.

- Evaluate Information Security –
 - What is the vendor doing to protect the data for both in and outgoing transmissions?
 - Firewalls
 - Traffic Flow Filters
 - Content Filters
 - Anti-Malware
 - Data Loss Detection / Prevention
 - What is done to test and what is used/measurements to determine passing secure environment?
 - Did the vendor have an independent third party audit their security? If so, ask to review that third party audit report.
 - What proactive security monitoring systems does the vendor have in place (such as internal network traffic, employee actions on systems, intrusion detection/prevention, security information & event management– real-time analysis of security alerts)?
 - How are systems maintained to keep current with security threats?
 - What mechanisms does the vendor employ to ensure that one customer can not maliciously access another's data?
 - Does the vendor's solution encrypt your data at rest AND in transit?
 - What level of encryption do they employ?
 - Who has access to the encryption key (customer, vendor, key escrow)?
 - Does the vendor follow Federal Information Processing Standards (FIPS) 140-2 or other encryption standards?
 - Is the encryption key stored separate physical location from where the encrypted data is stored?
 - What identity and access management (IAM) standards does vendor follow?

Infrastructure/Security - All cloud service vendors are NOT created equally.

- Physical Security
 - How do you know the vendor is effectively securing against unauthorized physical access to the actual data center facility? You do not want just anyone to walk into the facility and be able to access the hardware/software physical environment. Need protection from and a plan for protecting against insider threats either malicious or unintentional.
 - What security policies and/or procedures does the vendor have in place? Do they have an incident response plan? How are these communicated to employees? How are these plans/processes maintained and tested (frequency, scenarios, etc)?
 - POSSIBLE contract clause to consider adding to the agreement: "Vendor's datacenters shall be housed in nondescript facilities. Physical access shall be strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access datacenter floors. All visitors and contractors must be required to present identification and are signed in and continually escorted by authorized staff."
 - Which vendor staff has data access?
 - How is that access granted? The vendor shall only provide access to customer data only to those vendor employees and subcontractors who need to access the data to fulfill vendor's obligations under this agreement.
 - Is access logged, monitored, analyzed?
 - How is that access rescinded for employee separations or role changes?
 - What background checks does the vendor conduct on employees and/or contractors?
 - How does vendor ensure staff are effectively trained regarding security policies and practices?
 - Need to ensure that no one employee can unilaterally breach security and go undetected. What practices does the vendor employ to ensure appropriate segregation of duties?
 - Does the vendor require third parties to adhere to the same security policies? How does the vendor ensure such compliance?
- Operations Management
 - How do you know the cloud vendor is managing their data center with current and effectively configured systems? (NOTE: their failure to do so could diminish your access to their services and subject your data to damage, corruption or loss.) EX: a data center failed to switch to backup generators, depleted the energy in its UPS and shut down hardware in the region.
 - What are the vendor's asset inventory and management polices and processes?
 - What patch management mechanisms are employed to ensure rapid patching of device, application and systems vulnerabilities?
 - Does the vendor have media disposal policies and procedures? What does it include? (NOTE: if the vendor does not appropriately dispose of media containing customer information, your data could be exposed).

- Are disks logically wiped? How and by whom? Is media destroyed and by what process?
- Does the vendor have documented change management processes/procedures for handling system infrastructure upgrades? How are they reviewed and tested?
- Be aware of any upgrade or downgrade charges for exceeding or discontinuing a level of service and how such is measured. Pay as you go subscriptions makes it difficult to predict what the payment stream will be (budgeting for a year is undeterminable if you have unpredictable peaks of utilization). Moreover if you under or over estimate your utilization of cloud services you may be charged with unexpected upgrade/downgrade fees.
 - What mechanisms does the vendor employ to effectively manage and limit access to application/program source code?
 - What fire prevention/suppression mechanisms does the vendor employ?
 - Does the vendor have redundant power sources and back-up generators?
 - POSSIBLE contract clause: "The vendor shall agree to allow customer and customer contractors to perform remote security scans of the cloud services environment, subject to mutually agreeable scope and scheduling. The vendor will, in consultation with customer, identify and promptly implement any remedial measures necessary to address vulnerabilities or errors. Correction of vulnerabilities and errors will be performed by the vendor without separate or additional charge."
 - Does the vendor have a well defined Disaster Recovery (DR)/Business Continuity (BC) plan?
 - Does the vendor follow BC Standards (ISO 22301, ASIS SPC.1-2009, NFPA 1600:2010)?
 - Is there ongoing level of uninterrupted service?
 - Does it include regular offline backups?
 - Have the DR/BC plan been tested? How often?
 - Is there a DR/BC for 3rd Party Failures?
 - Who has the right to declare a disaster?
 - What circumstances warrant such a declaration?
 - What are the repercussions of making such a declaration?
 - **NOTE:** Force Majeure clauses (ACTS of God) should be SEVERELY restricted or deleted thus forcing the vendor to take more responsibility to be prepared for such ACTS of God or malicious threat circumstances such as having the ability to switch to other off-site data centers/fail over sites. Be sure that the off-site/failover site is equivalent to the primary site in environment and capacity.
- Is the failover site have sufficient geographic separation (at least 100 miles distance between sites)
- Is the failover site hot (A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment) or cold (A cold site is a similar type of disaster recovery service that provides office space, but the customer provides and installs all the equipment needed to continue operations. A cold site is less expensive, but it takes longer to get an enterprise in full operation after the disaster)?
- Is the failover site included in the subscription costs or is this an additional charge?

- What level of service will be provided at the failover site?
 - What is the vendor's obligations to notify customer regarding loss of service due to disaster? Notice provision timeframe? What details are to be included in such notice?
 - What is the vendor's obligations to investigate and conduct root cause analysis and vendor's obligations to correct underlying problem r resulting from disaster?
 - What is the timeframe for service restoration?
 - What is the vendor's remedy obligations to customer if data is lost or damaged? Is there reimbursement of costs related to any lost/ damaged data?

Service Level Agreements

- Parameters
 - Availability – define the time during which the service is functional and accessible by the customer (operational uptime). The following table shows the translation from a given availability percentage to the corresponding amount of time a system would be unavailable per year, month, or week.

Availability %	Downtime per year	Downtime per month*	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.8 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes

- Performance/Response Time – define the speed of an element(s) of the service
- Support/Error Correction
 - Days/Times of Access (8 hours a day by 5 days a week; 24 hrs a day x 7 days a week x 365 days)?
 - Support personnel qualifications? Does the vendor provide level 1 and/or level 2 help desk support? Or Is there dedicated support personnel specifically assigned to the Customer?
 - Where is the support personnel located?
 - How are issues prioritized and what are the resolution timeframes?
 - When is scheduled maintenance downtime performed? You will want to make sure that scheduled downtime does not occur during your peak utilization. How much advance notice are you given for such scheduled maintenance downtime?

- Latency – how long does it take for the data to travel between end user device and to the cloud data center? This is challenging because neither party controls the Internet.
- Metrics
 - Aspects of performance to consider are: (ask the vendor for this information)
 - Quantity of Incidents
 - Severity of Incidents (level of immediate harm, reputational damage, long term impact)
 - Time between incidents
 - Timeliness of Incident Reporting
 - Incident resolution time

- Service Thresholds

- Things to consider
 - How critical is it for the service to be available during certain dates/times?
 - How critical is it for the service to be available for a given percentage of time? – Refer to availability table on the previous page.
 - How critical is it for the service to recover quickly from any service failure?

NOTE: Keep in mind that Internet downtime could further reduce your access to the data/applications you have in the cloud.

- Reporting

- How is performance reported?
 - Real-time? Using vendor monitoring tools or third party audit?
 - Regular reports based upon vendor's log data?
 - Incident based reporting? Is this report done by the vendor or end user?

Consideration: Can you trust the vendor to self-report? Do you have the resources and/or tools to track performance on the service provided to you?

- Remedies

- What triggers a remedy? Performance degradation vs. complete outage? On what timeframe (real-time or cumulated over a month)?
- What is the remedy? Money refund, credit on future service?
- Goal is to get good services, NOT credits

NOTE: If you have an annual pre-paid (advanced paid) subscription then waiting for a credit on an annual renewal is NOT effective especially if you may not want to renew. So better to get money refund paid in real-time.

- Include in the contract a requirement for a Root Cause Analysis (RCA) to be conducted after an error or incident. Focus on identifying source of problem instead of simply mitigating symptoms. The goal is to prevent recurrence.
- Include provisions that if the vendor fails repeatedly in meeting service level performance then the vendor may be disqualified from future contracts.

NOTE: The agency will be required to submit a Vendor Performance Report (VPR) prior to any disqualification of a vendor from future contracts. Vendor Performance Reports (VPRs) are used for reporting vendor performance. The information in VPRs may be used as documentation for the suspension/debarment process.

- ▶ The procedure is as follows: The agency begins the process by completing the top section of the VPR and forwarding a copy to both the vendor and OSP. Note: If the contract or purchase order (PO) was issued by another state agency, the VPR should be directed to the agency procurement official (APO) or procurement agent (PA) of the agency that issued it. This should be accomplished in a timely manner (no more than two weeks after the occurrence). Then it is the vendor's responsibility to respond to the report by describing a proposed solution or taking exception to the report. The vendor has seven (7) calendar days to respond. The response is to be sent directly to OSP, the APO or PA. If OSP, the APO or PA does not find the response to be adequate or acceptable, the vendor may be requested to come to OSP or the agency for a meeting with the director, the APO or PA and an agency representative. If a mutually agreeable solution cannot be reached, the director of OSP, the APO or PA may hold the vendor in breach of the contract. The VPR form may be found at: <http://www.dfa.arkansas.gov/offices/procurement/Documents/VendorPerformanceReport.pdf>

Data Protection, Access & Location

- Ownership of Data
 - Affirm that your organization owns its data to include the results of any processing of your data as well as the vendor's log data as to who accessed service and when.
 - Restrict vendor's utilization of your data to operation of services and for no other reason (i.e., the vendor may not display or use your data or reference you as a client in any advertising). The vendor shall not provide any data mining unless contractually obligated to do so by the customer.
 - Data mining is sorting through data to identify patterns and establish relationships. Data mining techniques are used in a many research areas, including mathematics, cybernetics, genetics and marketing. Web mining, a type of data mining used in customer relationship management (CRM), takes advantage of the huge amount of information gathered by a Web site to look for patterns in user behavior.
 - POSSIBLE contract clause: The parties agree that as between them, all rights, including all Intellectual property rights, in and to customer data shall remain the exclusive property of customer, and vendor has a limited, nonexclusive license to access and use these data as provided in this agreement solely for the purpose of performing its obligations hereunder. All customer data created and/or processed by the services is and shall remain the property of the customer and shall in no way become attached to the services, nor shall the vendor have any rights in or to the data of customer.

- Data Access/Disposition

As stated previously, moving your data to a cloud service increases your dependence on the vendor. If you do not maintain the ability to move data to a different service, the cloud vendor gains leverage over you at negotiation time (i.e., you are then locked into that vendor dependent upon that vendor's good will to provide you with the level of services you need at a fair price when the vendor has no incentive or motivation to do so because the vendor knows you cannot easily transition to another service provider without significant costs and downtime in services.)

NOTE: Be aware of whether the outsourced applications are entirely proprietary (exclusive to that vendor) because this makes it difficult for the customer to transition to another cloud provider (you cannot readily load or move to a different provider due to incompatibility with other applications). Therefore seek open source solutions when feasible.

If you have a dispute with the vendor you are dealing with and that vendor denies you access to your data, to the outsourced applications are you able to operate your business without that vendor for a period of time?

NOTE: A subscription license for software applications and services is based on the right to access that software/services so long as you continue to pay the subscription fee. Once you stop paying the subscription fee your right to access and utilize that software/services stops. Be sure you have a transition plan in place to move off the cloud to either another provider or to bring that software/service in-house as part of your contract provisions (think ahead to have contractual obligations for the vendor to provide you with your data in an electronic format that can easily be downloaded/transferred to another location). Transitioning to an alternate provider is a costly endeavor as well as time consuming. A solid transition plan helps mitigate the risks and expense.

Therefore plan in advance how to switch to a different service provider with the following areas for planning considerations:

- Process
- APIs
- E-Discovery – require data to be preserved, collected, and produced in a timely manner for legal disputes and Freedom of Information Act (FOIA) requests. Need to make sure that the vendor shall be required to expedite retrieval of all data associated with an E-Discovery claim at no additional cost/charge to do so.
- Timeframe that the vendor has to supply you with your complete data
- Format of data to be returned to you
- Testing the data returned to you to verify that it is complete and has maintained its data integrity in the transfer process (i.e., did not get corrupted or degraded).
- Destruction – the vendor should be required to destroy their copy of your data AFTER they have transferred your data to you and you have had the opportunity to verify that the copy of the data provided to you is intact and complete.
 - Specify timeframe that the vendor must destroy their copy of your data
 - Require the vendor to certify in writing that your data has been destroyed and describe in what manner it was destroyed
 - Provide a provision that allows you the right to audit the vendor's compliance with the destruction of your data.

- POSSIBLE contract clauses:
Upon request by customer made before or within sixty(60) days after effective date of termination and at no additional cost to the customer, the vendor shall make available to customer a complete and secure (i.e., encrypted and appropriately authenticated) download file of customer data in XML format including all schema and transformation definitions and /or delimited text files with documented, detailed schema definitions along with attachments in their native format.

The parties agree that on the termination of the provision of data processing services, the Vendor shall, at the choice of the customer, return all the personal data transferred and the copies, including backup copies, thereof to the customer or shall destroy all the personal data and certify to the customer that it has done so. The vendor warrants that upon request of the customer and/or the supervisory authority, it will submit its data processing facilities for an audit of the measured referred to above.

- POSSIBLE contract clause: Prohibition of electronic self-help: The contractor agrees that in the event of any dispute with the customer regarding an alleged breach of contract, the contractor **shall not** use any type of electronic means to prevent or interfere with the operation of or customer access to the system/services, without first obtaining a valid court order authorizing same. The customer shall be given proper prior written notice (e.g. a minimum of seven days advance notice) and an opportunity to be heard in connection with any request for such a court order. The contractor understands that it is foreseeable that a breach of this provision could cause substantial harm to the customer. No limitation of liability, whether contractual or statutory, shall apply to a breach of this paragraph.

- Data Breaches

Your data in the cloud could be inappropriately or maliciously accessed. Who will be responsible for what associated follow-up actions and/or expenses?

- Indirect costs:
 - Public Relations – reputational damage control costs (press releases, call centers, social media)
 - Staff – reassignment to fix breach issues plus data compromise distraction which results in lost productivity
 - Government Investigations – resources (legal, etc) to respond to inquiries
- Key vendor obligations in breach situations:
 - Notification to customer (including timeframe). NOTE: you may want to indicate that ANY data breach whether it is your specific data or that of another customer's data that you receive notification that such has happened and still be informed of what measures are being taken to correct the situation and prevent such from happening again.
 - Details (circumstances, type of data that was breached, etc)
 - Corrective Action(s) to be taken
 - Investigations/Root Cause Analysis – make sure this breach situation does not happen again
 - Indemnification - To compensate for loss or damage incurred by the customer.

- Cyber-Risk Insurance: Vendor to provide an errors and omissions policy that names the customer as a beneficiary (i.e. name customer as an additional insured) and that covers various types of Internet-based risks, including cloud-based risks such as security and privacy liability, computer security, data and information, business interruption, cyber-extortion, cyber forensics. Customer should require certificates of insurance. Coverage amount should be adequate to cover vendor's total liability due to a breach. **NOTE:** The average total cost of breach in the U.S. is \$214 each compromised record and potentially \$7.2 million per breach event.
 - One of the benefits of cyber-risk insurance is that an insurer's willingness to insure a vendor can serve as a their party verification of that cloud vendor's infrastructure/security because the insurer is unlikely to insure a cloud vendor who represents a high risk of loss.
- POSSIBLE contract clause: Vendor shall report any confirmed or suspected breach to customer immediately upon discovery, both orally and in writing, but in no event more than two (2) business days after vendor reasonably believes a breach has or may have occurred. Vendor's report shall identify: (a) the nature of the unauthorized access, use or disclosure, (b) the protected information accessed, used, or disclosed, (c) the person(s) who accessed, used, and disclosed and/or received protected information (if known), (d) what vendor has done or will do to mitigate any deleterious effect of the unauthorized access, use or disclosure, and (e) what corrective action vendor has taken or will take to prevent future information, including a written report, as reasonably requested by customer.
- Locations of Data:
 - Your data may be in data centers in multiple locations around the world. Data may pass through other countries in transit. If the vendor you are dealing with subcontracts any portion of the services are you okay with whomever the subcontractor will be – even if the company is headquartered overseas? Know WHERE your data will be. Be sure to include provisions that your data must reside within the United State of America and no event be transferred or accessed by outside of the continental U.S.
 - Identify/Restrict data center location(s)

NOTE: Location of data center(s) can impact performance (latency/response time). Distance from both point of usage, as well as major network hum impacts Internet performance.
- Legal Requests for Access to Data
 - With in-house systems, should your data be subject to a subpoena or other legal request for access, you have more direct control in managing its release. Should your data in the cloud becomes subject to such a request for access, your data could be released without your knowledge! To mitigate the associated risks, contractually detail the vendor's obligations in these circumstances:
 - Notify customer upon receipt of request and prior to providing access
 - Cooperate with customer efforts to appropriately manage release
 - Limit any release to the extent possible, and to the minimum required by law

- Provide customer copy of vendor's response
- Codify any existing vendor policy in contract (i.e., be sure that the standard practice for handling legal requests for data by the vendor is stated and explicitly defined within the contract).
- POSSIBLE contract clause: Where a receiving party is required to disclose the confidential information of the disclosing party pursuant to the order of a court or administrative body of competent jurisdiction or a government agency, the receiving party shall: (i) if practicable and permitted by law, shall notify the disclosing party prior to such disclosure, and as soon as possible after such order; (ii) cooperate with the disclosing party (at the disclosing party's costs and expense) in the event that the disclosing party elects to legally contest, request confidential treatment, or otherwise attempt to avoid or limit such disclosure; and (iii) limit such disclosure to the extent legally permissible.

Vendor Relationship

- Initial Set-up Costs vs. On-going/Recurring Costs:
 - Vendors will typically try to get customers to focus on initial buy-in costs then apply "list price" to continue or expand usages after initial term. To protect against this you have to consider:
 - Renewal price caps be tied to a specific percentage increase (such as 3%) or the cost of list price whichever is lesser (over time technology costs may decrease).
 - No dollar increases if volume decreases. There should be no minimum purchase volume nor multi-year commitments.
 - Must protect against the vendor charging new or increased fees or charges. Indicate that the provision of services in the current configuration is provided at a firm, fixed rate and shall not increase unless there is an increase in services ordered by the customer.
- Termination: Keep Termination Decision in Your Control.
 - Restrict vendor termination rights to triggering events (ex. Significant threat to security/integrity of infrastructure) but also include customer opportunity to cure.
 - Be sure that any Vendor termination requires a minimum of six (6) months advance written notice. Vendor termination must not be allowed for legitimate payment disputes. Maintain your right to terminate services with 30 days prior written notice to the vendor.
- Product/Service Functionality:
 - Many contracts only state a product/service's name without say specifically what it does. Be sure to include a description of the functionality of the services being acquired because otherwise a product name change could result in losing access to key functionality.
 - Keep in mind that Cloud Computing is always updating functionality / services. Functionality can be added or deleted at any time. Be sure to get advance notification of any deletions/changes to services. The notification period should be sufficient time to allow you to switch cloud service providers should you not like the changes being made.

- Be aware that the vendor could force you to replace /switch to other substituted services. You should be sure to include your right to replacement products providing similar functionality under a new name.
- POSSIBLE contract clause: Preserving rights to system functionality: In the event that the contractor deletes functions that were mandatory requirements of the existing contract for cloud services from the licenses system and offers those functions in other or new system products, the portion of those other or new products which contain the functions in question, or the entire product, if the functions cannot be separated out, shall be provided to the customer under the term of their subscription license along with any applicable modifications necessary to make the product operate with the licensed system, at no cost to the agency and shall be covered under the subscription license at no cost to the agency.
- Mergers and Acquisitions:
 - IT companies are often bought out by or merged with other companies.
 - It is critical that there is a contract assignment clause that stipulates the contractor shall not transfer any interest in the contract, whether by assignment or otherwise, without the prior written consent of the customer.
 - Consent to assignment shall only be granted when the assignee agrees to be bound by all of the terms and conditions of the contract agreement and the assignee operates the business as a continuation of such party's business.
 - Any assignment of moneys shall be void and ineffective to the extent that such assignment attempts to impose upon the customer obligations to additional payment of such moneys, or to preclude the customer from dealing in all matters pertaining to the contract agreement including, but not limited to, the negotiation of amendments or the settlement of charges due.
- Vendor Outsourcing:
 - Cloud services typically do involve provisioning out/subcontracting to third party vendors. Regardless of third party subcontractors be sure that the contract stipulates that the primary vendor shall remain responsible for all service performance matters.
 - POSSIBLE contract clause: Vendor may subcontract in whole or in part the services detailed in his agreement provided that the vendor remains solely responsible for the performance of its obligations under this agreement.
 - Be sure that the cloud service contract agreement is govern by the laws of the state of Arkansas and that the legal venue for any legal claims or litigations shall be held in Pulaski County, Arkansas.
 - Typically the vendor's Terms and Conditions are provided online where you have to "click" to agree to their terms and conditions in order to access their site. Do NOT agree to reference a vendor's URL website terms, provisions, and conditions. The vendor can unilaterally change those terms and conditions without notice and without your expressed written approval. Instead print out the website terms and negotiate them making the modified contract agreement an inclusion to the cloud service agreement indicating that the exhibit supersedes and governs in the event of conflict with the vendor's URL website terms and conditions.

- Technical Support:
 - The vendor's technical support and training provisions should be described in the contract.
 - Indicate who can access support.
 - Days/Hours of support coverage availability
 - How or manner in which the customer may access support
 - What is the defect/error correction process (bug fixes)
 - What is the escalation process to resolve issues
 - Require various access channels in the contract (i.e., via multiple web browsers, mobile devices, etc) as well as the vendor providing advance notice to customers of any changes.
- Cloud Escrow:
 - What if the cloud vendor ceases business operations such as due to bankruptcy? If you lose the data are you ok with that? Suggest including escrow language in your contract.
 - Deposit source code, data, documentation and all other necessary and available information that would assist the Customer in the reconstruction, maintenance or enhancement of the material.
 - Verification of deposits from escrow agent
 - Updates deposits regularly
 - Trigger events (bankruptcy, violation of contract including technical support)
 - Temporary hosting services – ex. Iron Mountain SaaS Protect Escrow includes up to 60 days of hosting in addition to code and data escrow
 - Timeframe for release of escrowed materials

*The majority of the material presented is from the following source:
Cloud Computing Risk Mitigation ~ Author Mr. Thomas Trappier, Director of UCLA Software Licensing