V.2019.01.08.1

Arkansas Cloud Strategy

Table of Contents

Published:	January 28, 2019
Revisions:	
Review Frequency:	Annually
Last Reviewed:	

Executive Summary

The expanded presence of cloud computing in the state enterprise IT landscape is the direct result of the increased need for agility, scalability and business continuity. The potential cost, agility, and operational advantages of cloud computing and its significant potential impact upon every aspect of IT compels organizations to incorporate it into IT modernization plans. Understanding the value cloud services represent and how the value can be realized is important. Insight into best practices and guidelines for protecting the agency and the state could benefit organizations entering into individual formal agreements.

Although there are current instances of cloud services in use, this is primarily the outcome of the procurement of a specific software solution, and not an outcome of an enterprise wide initiative that capitalizes upon of the inherent and desirable characteristics offered by cloud computing. Given ongoing efforts for statewide data center optimization and improvements to be realized under varied enterprise software agreements, Arkansas must position itself to leverage the potential benefits of cloud computing from an enterprise view. To this end, Arkansas is proceeding with a “cloud right” policy. New services, applications and major revisions to existing ones will be evaluated to determine whether a cloud versus on-premise deployment is possible and in the best interest of the state.

Pursuant to this goal, it must be recognized that not all applications are suitable for external cloud solutions. For example, many legacy applications are simply unsuitable for deployment to the cloud. Old and vulnerable coding with known security vulnerabilities have shown that hammering legacy applications into a modern virtualized environment is not a good fit. A balance between cloud and on-premise infrastructure must be achieved to ensure services are available to Arkansans in the manner that is in the best interest of the state.

This document is to serve as both guidance in how to best utilize cloud services and as governance for the contractual terms and conditions under which they are provided.

Arkansas Cloud

Cloud Services Defined

At its core, cloud computing technologies encompass an operational expense (OpEx) or 'Pay as You Go' model, allowing the consumer of the resources to scale up or down as desired. In practice, cloud computing is a term that has evolved to mean many different things, from raw storage or compute platform resources to fully provisioned and managed software solutions.

Arkansas is following the National Institute of Standards and Technology (NIST) definition of cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

- *On-demand self-service*: A consumer can unilaterally provision computing capabilities as needed automatically without human interaction.
- *Broad network access*: Capabilities are available over the network through heterogeneous thin or thick client platforms.
- *Resource pooling*: Computing resources are pooled, and potentially shared among multiple tenants, with resources often virtualized and dynamically assigned and reassigned in accordance with customer demand. There is location independence in that the customer generally has no control over the exact location of provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).
- *Rapid elasticity*: Capabilities can be elastically provisioned and released to scale rapidly commensurate with demand.
- *Measured service*: Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models

- *Software as a Service (SaaS)*: The capability provided to the consumer is to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based mail), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Platform as a Service (PaaS)*: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed

applications and possibly configuration settings for the application-hosting environment.
- *Infrastructure as a Service (IaaS)*: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

- *Private Cloud*: The Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- *Community cloud*: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- *Public Cloud*: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- *Hybrid Cloud*: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

ARCloud

In order to address agency needs for highly available, mission critical applications, the Arkansas Department of Information Systems (DIS) implemented and operates ARCloud as the state on-premise solution for Private Cloud hosting.

Currently, the shared services environment offers a mix of hosted services:

- Managed and unmanaged Windows virtual machine hosting
- Managed and unmanaged Linux virtual machine hosting (open source)
- Managed and unmanaged Linux virtual machine hosting (proprietary)
- Shared SQL Server hosting
- Shared DB2 hosting
- Shared Email hosting
- Shared collaboration application hosting
- Web hosting

Transformation of the IT Infrastructure Landscape

Cloud computing outlines a fundamental shift for Arkansas. The decentralized IT environment for the state has the same issues that many other organizations, including the federal government, have around infrastructure:

- Low asset utilization
- Fragmented demand for resources
- Duplicative systems
- Difficulty managing the disparate systems
- Long lead times for implementation
- Aging infrastructure and application platforms
- Resource constraints limit staying current with technology developments

Cloud computing can address many of these inefficiencies and improve service delivery to citizens. It can further create a more agile environment, to promote innovation and scalability.

As part of adopting a "cloud right" policy, Arkansas will look to evaluate cloud provisioning in new or expanded deployments of applications or services. Subsequently, existing applications will be evaluated for potential transitioning to a cloud platform. This will lead to potential efficiencies and will allow the state to take advantage of the research and development pursued by cloud service providers and the technological innovations that result.

Arkansas Cloud Strategy Goals

The Arkansas Cloud Strategy has four simple goals which are in alignment with provision of service in the best interest of the state.

- Reduce costs and redundancy
    - Increase hardware utilization
    - Reduce data center footprint
    - Recognize and reduce duplication in environments
- Increase agility
    - Simplify management of the environment
    - Increase procurement efficiency
    - Improve scalability and elasticity
- Continuously improve
    - Take advantage of innovations in optimizing infrastructures for service delivery
    - Rapidly adopt improvements in applications
- Reduce business, operational and security risk
    - Ensure ongoing service levels for operations, security and monitoring
    - Take advantage of specified time frames for incident resolution and refined processes for root cause analyses

Decision Framework for the Arkansas Cloud Strategy

Determining the Appropriate Deployment Model

Identification of the appropriate cloud deployment model should be given careful consideration as to security risk and service availability when analyzing options for service migration to cloud options. Government services revolving around non-substantive communication and non-sensitive data dissemination are perfect candidates for public cloud offerings. Extreme care should be taken when considering moving sensitive data (such as PII, HIPAA, FERPA, PCI, FTI, SSA, CJIS) into a public cloud offering. When analyzing the potential benefits balanced by the potential risks, consider the factors outlined below when evaluating the different deployment models for a particular initiative.

Public Cloud

In general, a public cloud offering should maximize or ensure that the following considerations are addressed:

- *Efficiency*: The public cloud offering should decrease the financial burden on the state and should be significantly more cost efficient than other delivery models.
- *Agility*: The public cloud offering should allow a faster time to market than other delivery models.
- *Security*: The public cloud offering should meet the security requirements for the initiative.
- *Technology Lifecycle*: The public cloud offering should replace hardware/software currently in use by the government that is at end of life.

The following requirements should be mandatory for any public cloud offering under consideration:

- ✓ Data must be stored in the United States.
- ✓ A vendor breach response process should be specified in the agreement to address any security related unauthorized access or loss of data.
- ✓ An exit strategy allowing data export in the event of contract termination.
- ✓ A vendor data disposal process should be specified in the agreement.
- ✓ Vendor must be in compliance with state security policy.
- ✓ Vendor agreement must state Arkansas owns the data.
- ✓ The legal jurisdiction for an agreement under which these services are provided must be Arkansas.
- ✓ Bandwidth must be available into the government agency for consumption of the public cloud service.

Private Cloud

In general, a private cloud offering should maximize or ensure that the following considerations are addressed:

- *Security*: The private model should provide for better information security when security risks are identified with a public cloud offering that cannot be overcome.
- *Technology Readiness*: Bandwidth is available if the delivery model into the government agencies and services is from an external source.
- *Efficiency*: The model should provide for 'on demand' scaling, or the hardware exists on premise.
- *Technology Lifecycle*: The hardware should be vendor supported.

Hybrid Cloud

Under certain circumstances, a hybrid model can be utilized to address non-linear scaling needs, with public cloud resources being utilized to temporarily augment hardware resources of a private cloud typically utilized to provide services. In general, the model should maximize or ensure that the following considerations are addressed:

- *Efficiency*: The public cloud offering should decrease the financial burden on the state, and it should be significantly more cost efficient to pursue a hybrid model than adding hardware to the private cloud infrastructure.
- *Agility*: The public cloud offering should allow for faster implementation timeframes.
- *Security*: The public cloud offering should meet the security requirements for the initiative.
- *Technology Readiness*: The hybrid solution should allow for the network, hardware, and/or software to take advantage of the environment.

Community Cloud

The state is currently pursuing community cloud use in the form of 'government cloud' offerings under varied contract vehicles. Much like public cloud, economies of scale can be achieved via the pooling of state and local government resources in these cloud offerings. In general, the model should maximize or ensure the following considerations are addressed:

- *Efficiency*: The economies of scale should allow for a cost effective delivery model.
- *Innovation:* The community cloud offering should offer services not available outside of the community cloud.
- *Technology Readiness: Each entity within the community cloud should share like processes and can support the delivery model.*

Business Case for Deployment Model

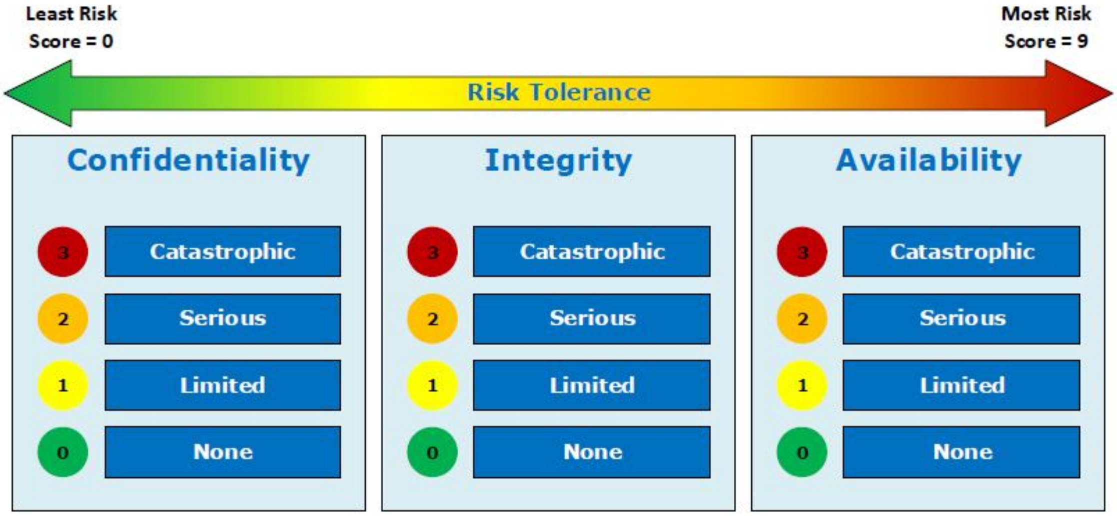
New or expanded deployments of applications or services should be evaluated and a business case developed for deployment in the cloud versus deployment on traditional on-premise infrastructure. As a general rule, three key components should be examined to determine whether cloud deployment is a viable option versus on-premise infrastructure, and if so, the cloud deployment model that would be most appropriate.

Workload Risk Assessment

Adopting NIST terminology for key components of computer security risk assessment, a workload under consideration for cloud deployment can be evaluated by the combination of metrics of 3 characteristics:

- *Confidentiality*: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- *Integrity*: Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. This has two components:
    - *Data Integrity*: The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
    - *System Integrity*: The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
- *Availability*: Ensuring timely and reliable access to and use of information.

The following graphic represents a mechanism to interpret workload risk assessment as a combined score to be used in the analysis workflow presented at the end of the "Business Case for Deployment Model" section.



Data Classification

For any data to be stored, the data should be classified in accordance with the state Data and System Security Standard (SS-70-001).

The standard is available at:

http://www.dis.arkansas.gov/Websites/dis/images/SS-70-001_dataclass_standard.pdf

The standard provides a framework through which data can be classified with respect to data sensitivity and data criticality. Guidelines for the classification of data in accordance with the standard are available at:

http://www.dis.arkansas.gov/Websites/dis/images/DataClassificationGuide.pdf

Data classification should be represented on the Data Classification Grid available at:

http://www.dis.arkansas.gov/Websites/dis/images/data_grid.pdf

The Data classification grid is also provided as Appendix A to this document.

Once data to be stored has been classified, the criticality and sensitivity level identified can be used in the analysis workflow presented at the end of the "Business Case for Deployment Model" section.

Cost Comparison

Cost between cloud deployment versus on-premise deployment should be compared. As to cost factors, beyond the obvious initial cloud service startup costs or on-premise capital expenditure, elements to consider which are sometimes overlooked include:

Cloud	On-premise
Ongoing labor support costs Migration services costs Data transfer and transaction costs Data storage costs Bandwidth increase costs	Ongoing labor support costs Hardware maintenance Software maintenance Ancillary software update costs Refresh cost (if applicable)

Depending on the specific service under evaluation for cloud deployment viability, cost analysis between various cloud deployment models may be appropriate.

Analysis Framework Workflow

After evaluation of the three key elements outlined in this section, the information can be utilized in the workflow provided as Appendix B to this document as a guide for cloud deployment viability and type.

In the case of some legacy applications, the software technologies utilized simply are not a fit for cloud architecture - licensing restrictions, cloud deployment voids vendor maintenance obligation, etc. In these scenarios, additional evaluation is required, and the costs of procuring a cloud compatible solution should be considered.

Procurement Considerations

When evaluating cloud options, regulations and standards governing your specific application versus the multitude of cloud services and service providers can create challenges in ensuring that adequate provisions are addressed in any service agreement such that cost, security, and performance risks are minimized. The four key areas below should always be considered.

- *Performance*: This can include availability, capacity, and elasticity elements of a cloud service.
- *Service*: This can include service monitoring, response time, resilience/fault tolerance, disaster recovery, data backup/restoration, and vendor support of the service.
- *Data Management*: This can include defining of vendor versus customer data, intellectual property rights, account data, derived data, portability of data, deletion of data, location of data, and examination of data.
- *Governance*: This can include accessibility, roles and responsibilities related to the service, handling of PII, information security, termination of service, changes to features and functionality, law enforcement access, and provisions for attestation, certifications, and audits.

Commonly, agreements for cloud service lack provisions which address the following issues in a manner favorable to the state:

- Provision for governing law to be the state of Arkansas
- Provision for service levels
- Provision for indemnification to the state
- Location of Data
  - Provision providing that data must reside within the United States of America
  - Provision providing that data will not be transferred outside of the United States of America
- Vendor Obligations in the Event of a Data Breach
  - Provision requiring specific vendor notification process to customers (including specific timeframes) that the breach has occurred.
  - Provision requiring vendor report on details of the breach. (i.e. circumstances of the breach, type of data compromised, who was impacted)
  - Provision requiring vendor statement as to what the vendor has done or will do to mitigate any deleterious effect of unauthorized access, use, or disclosure of the data.
  - Provision requiring vendor statement as to what corrective action the vendor has taken or will take to prevent future data breaches.
- Provision for data export for purpose of exit strategy
- Provision for data destruction by vendor after contract termination.

While this is not an exhaustive list, these elements should be considered mandatory for any vendor agreement for cloud services or even vendor hosted solution.

Any compliance or regulatory requirements that use of the service is subject to, or data stored or processed through the use of the service is subject to, must be identified. It is mandatory that the vendor attest and demonstrate that the service offered is compliant with those requirements identified. This includes, but is not limited to, security and audit requirements.

More detailed information about these areas of concern are included in Appendix C to this document. The appendix also addresses a lengthy list of legal topics and contract considerations to explore in relation to the provision of cloud services. Overall, these areas of consideration should apply not only to cloud service provider agreements, but any agreement for vendor hosted services, and should be examined carefully in pursuit of the goal of providing service in the best interest of the state.

Conclusion

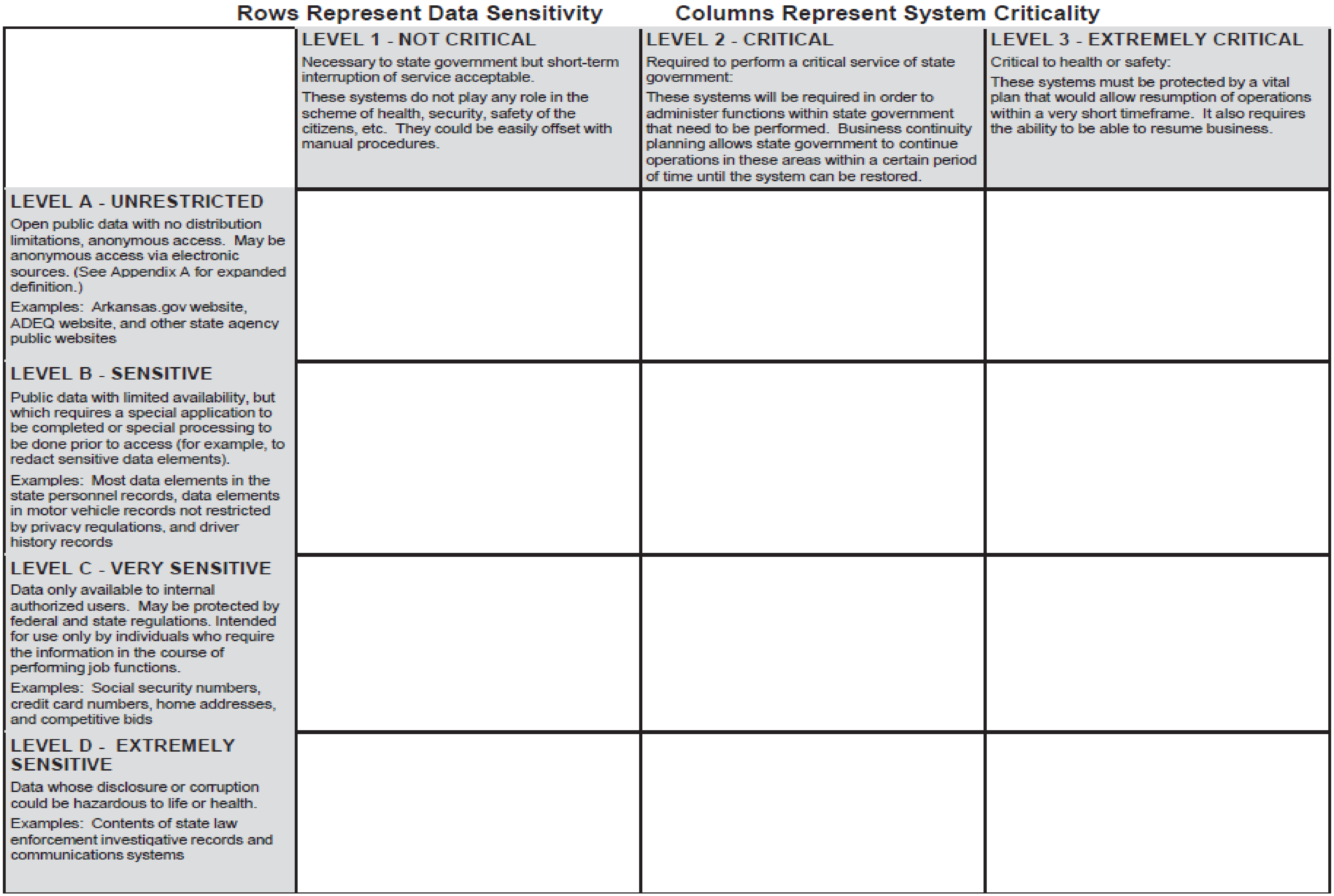
There are numerous opportunities for Arkansas to leverage cloud based technologies. It is important that the state's consumption of these services be governed and guided to avoid a simple replication of the current siloed IT infrastructure to a cloud environment and to effectively protect the information assets of the state. Arkansas Department of Information Systems (DIS) will take leadership for this governance in the following ways:

- *Standards*: As service offerings evolve to incorporate new standards, DIS will document these and other standards applicable to the efforts of migrating services to the cloud.
- *Business use cases*: DIS will provide guidance and assistance to agencies in developing cost comparisons, risk assessments, and overall business case development for migration of services to the cloud.
- *Procurement*: DIS will work with the Arkansas Department of Finance and Administration, Office of State Procurement to develop standard terms and conditions for cloud services contracts and participating addendums to cooperative contracts providing cloud services. Requests for procurement of cloud services will require DIS review and approval prior to execution of a contract.
- *Monitoring and Reporting*: DIS will provide guidance for monitoring of cloud services, to ensure anticipated benefits are being realized.

Appendices

- *Appendix A*: Data and System Security Classification Grid
- *Appendix B*: Analysis Framework Workflow
- *Appendix C*: Procurement Areas of Consideration
- *Appendix D*: Business Justification Template

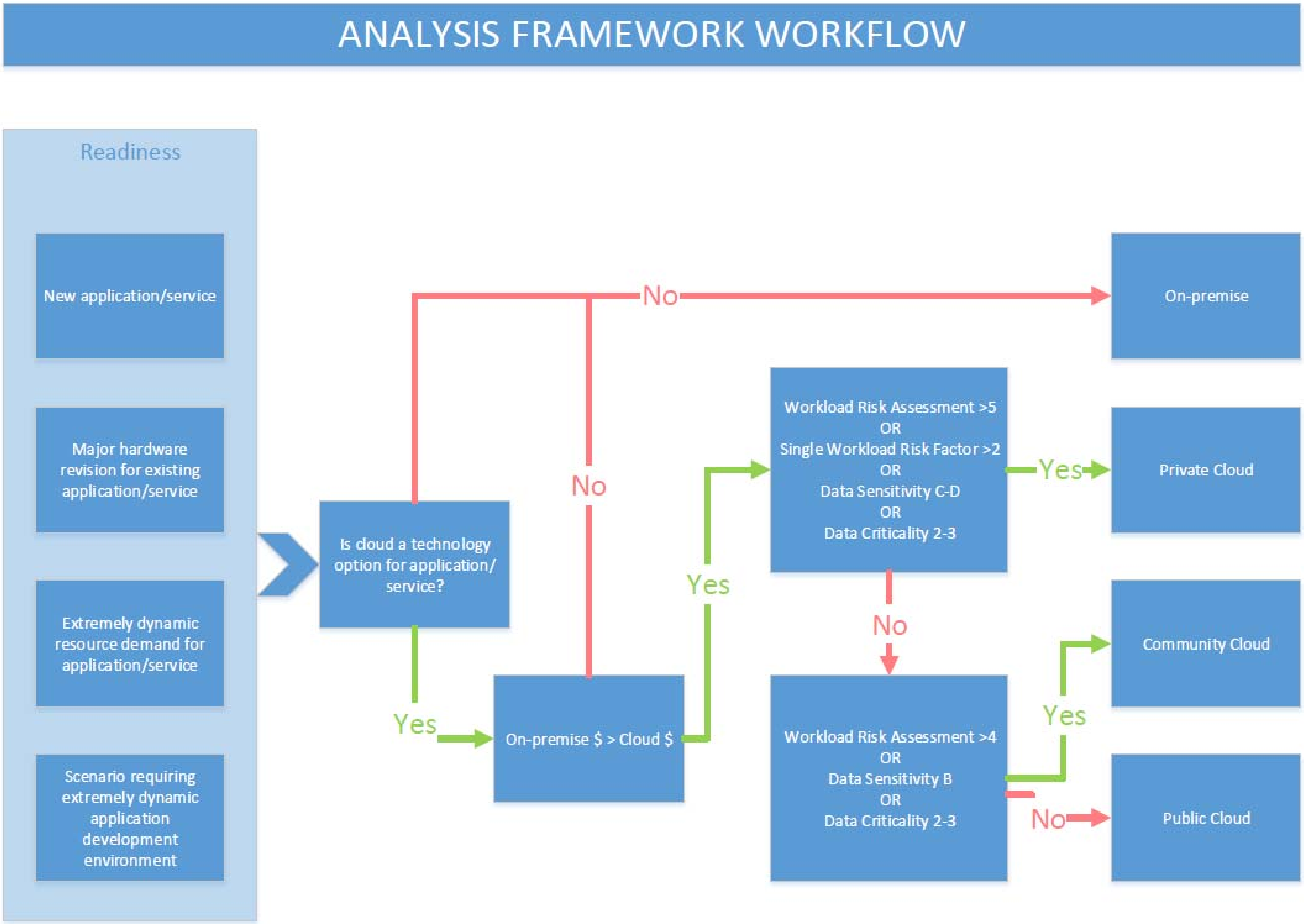
Appendix A: Data and System Security Classification Grid



Rows Represent Data Sensitivity Columns Represent System Criticality

	LEVEL 1 - NOT CRITICAL Necessary to state government but short-term interruption of service acceptable. These systems do not play any role in the scheme of health, security, safety of the citizens, etc. They could be easily offset with manual procedures.	LEVEL 2 - CRITICAL Required to perform a critical service of state government: These systems will be required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the system can be restored.	LEVEL 3 - EXTREMELY CRITICAL Critical to health or safety: These systems must be protected by a vital plan that would allow resumption of operations within a very short timeframe. It also requires the ability to be able to resume business.
LEVEL A - UNRESTRICTED Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources. (See Appendix A for expanded definition.) Examples: Arkansas.gov website, ADEQ website, and other state agency public websites			
LEVEL B - SENSITIVE Public data with limited availability, but which requires a special application to be completed or special processing to be done prior to access (for example, to redact sensitive data elements). Examples: Most data elements in the state personnel records, data elements in motor vehicle records not restricted by privacy regulations, and driver history records			
LEVEL C - VERY SENSITIVE Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by individuals who require the information in the course of performing job functions. Examples: Social security numbers, credit card numbers, home addresses, and competitive bids			
LEVEL D - EXTREMELY SENSITIVE Data whose disclosure or corruption could be hazardous to life or health. Examples: Contents of state law enforcement investigative records and communications systems			

Appendix B: Analysis Framework Workflow



ANALYSIS FRAMEWORK WORKFLOW
Readiness
New application/service
Major hardware revision for existing application/service
Extremely dynamic resource demand for application/service
Scenario requiring extremely dynamic application development environment
Is cloud a technology option for application/ service?
No
On-premise
No
Yes
On-premise $ > Cloud $
Yes
Workload Risk Assessment >5 OR Single Workload Risk Factor >2 OR Data Sensitivity C-D OR Data Criticality 2-3
Yes
Private Cloud
No
Workload Risk Assessment >4 OR Data Sensitivity B OR Data Criticality 2-3
Yes
Community Cloud
No
Public Cloud

Appendix C: Procurement Areas of Consideration

Four Key Areas

When evaluating cloud options, regulations and standards governing your specific application versus the multitude of cloud services and service providers can create challenges in ensuring that adequate provisions are addressed in any service agreement such that cost, security, and performance risks are minimized. The checklist below can be aligned with specific policy and regulatory requirements to aid in this effort.

Performance

Availability	o The percentage of time that the service is available and usable
Capacity	o The number of simultaneous connections o The maximum capacity of resources o The number of inputs that will be processed over a period of time o The amount of data that will be transferred over a period of time
Elasticity	o How fast and precisely the service can adjust to the amount of resources that are allocated

Service

Service Monitoring	o The parameters and mechanisms to monitor the service
Response Time	o The maximum, average, and variance in response time
Service resilience/fault tolerance	o The methods used to facilitate resilience and fault tolerance (include mean times, maximum times, and units of measurement)
Disaster Recovery	o The maximum time required to restart the service in outage o The maximum time prior to a failure during which the changes may be lost o The recovery procedures to restore the service and data
Backup and Restoration of Data	o The number of data backups made in a period of time o The methods of backup and backup verification o The backup retention period o The number of backups retained o The location of backup storage o The number of restoration tests and the availability of test reports

	o The alternative methods for restoring data
Cloud Service Support	o The available support plans, associated costs, and associated hours of operation o The specific contacts for service support o The service support methods (phone, web, tickets, etc.) o For incident support: the incident support hours, levels of support, response time (average and maximum), reporting methods, and notification terms.

Data Management

Define Provider versus Customer Data	o Define Cloud Service Provider data. o Define Cloud Service Customer data.
Intellectual Property Rights	o Describe any intellectual property rights the cloud service provider claims on cloud customer data and vice versa.
Account Data	o List the required account data fields (names, addresses, etc.).
Derived Data	o Define the types of derived data and policies for use/access
Data Portability	o Data portability capabilities including methods, formats, and protocols.
Data Deletion	o Define the minimum and maximum times to completely delete cloud service customer data. o Describe the deletion process. o Describe the data deletion notification policy.
Data Location	o List the geographic locations that data may be processed and stored, and if the cloud service customer can specify location requests.
Data examination	o Describe how the cloud service provider examines cloud service customer data.

Governance

Accessibility	o List accessibility standards, policies, and regulations met by the service.
Roles and Responsibilities	o The roles and responsibilities for the parties.
Personally Identifiable Information	o The PII protection standards met by the cloud service provider.
Information Security	o The information security standards met by the cloud service provider.

Termination of Service	o The process of notification of service termination, including the length of time that data and logs are retained after termination, the process for notification, and the return of assets.
Changes to Features and Functionality	o The minimum time between service change notification and implementation, and service change notification method. o The minimum time period between the availability of a feature/function and the deprecation of that feature/function.
Law Enforcement Access	o The policy for responding to law enforcement requests of cloud service customer data.
Attestation, Certification, and Audits	o List/define the standards, policies, regulations, and applicable certifications that the cloud service provider attests to. Include audit schedule and location policies.

Legal Issues

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, determine if the applications were 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, 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 cyberattacks. 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.

Questions and Considerations for Contracts

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.

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 measured to determine passing secure environment?
  - 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.”
  - 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 cannot 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?

- **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 policies 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 overestimate 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?

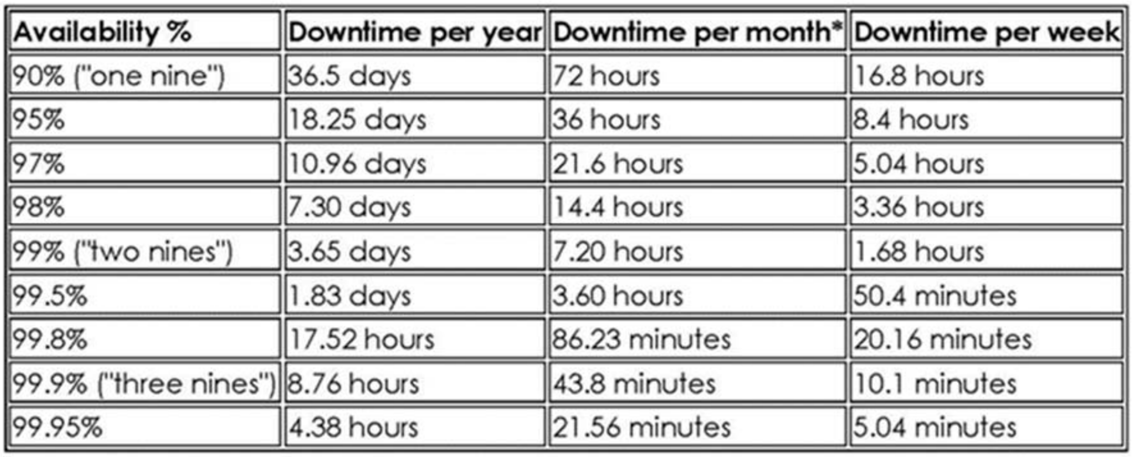
- **Disaster Recovery/Business Continuity**
  - Does the vendor have a well-defined Disaster Recovery (DR)/Business Continuity (BC) plan?
  - Does the vendor follow BC Standards (ISO 22301, ASIS SPC.1-2009, NFPA 1600:2010)?
  - Is there ongoing level of uninterrupted service?
  - Does it include regular offline backups?
  - Have the DR/BC plan been tested? How often?
  - Is there a DR/BC for 3rd Party Failures?
  - What fire prevention/suppression mechanisms does the vendor employ?
  - Does the vendor have redundant power sources and back-up generators?
  - 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.
  - Does 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 hours 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 endues 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**
    - 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 in this 'Service Level Agreements' section.
    - 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?
        - 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: Agencies 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. For more information about the VPR process, please see the DFA-OSP website at:
      http://www.dfa.arkansas.gov/offices/procurement/Pages/VPR.aspx

Data Protection, Access and Location

- **Ownership and Use of Data**
    - Affirm that your organization owns the data, including 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 for transition
- 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:
    - 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 inquires
  - 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 third 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.

    - The scenario of what constitutes a Data Breach should be clearly defined within the contract.
      POSSIBLE definition: A Data Breach is any unauthorized release, duplication, accessing, transmittal, or modification of customer data, in whole or in part, for any reason.
    - 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 hub 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 saying 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.
  - POSSBILE contract clause: Vendor may subcontract in whole or in part the services detailed in this agreement provided that the vendor remains solely responsible for the performance of its obligations under this agreement.

- **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

- **Terms and Conditions of Contract**
  - Be sure that the cloud service contract agreement is governed 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.

Appendix D: Business Justification Template

General Information

Description of Purpose and Scope
(enter description)

Define the specific business need that drives the investment. Account for both current and future needs. State how the proposed investment aligns with business and strategic objectives.

Description of Target Customers or Users
(enter description)

Readiness

Question	**(select)**
Is this a new application or service?	
Is this a platform hardware refresh for an exising application or service?	
Does this application or service have extremely dynamic resource demand?	
If this is an existing application or service, has licensing been evaluated for cloud deployment?	
If this is an existing application or service, has verification that there is no voiding of applicable vendor maintenance/support agreement occurred?	

Deployment/Use Timeline

	(enter date - mm/dd/yyyy)
Start of deployment effort	
End of deployment effort	
	(select)
Is this anticipated to be a temporary or ongoing need?	
	(enter approximate months)
If temporary, how many months?	

Technology Solution

Item	**(enter description)**
Vendor	
Describe the solution	

Management of Initiative

Management Methodology

Summarize the methodology used to manage the initiative in each of the following areas:

Item	**(enter description)**
Resources Required	
Reporting Requirements	
Performance Criteria	
Budget Reporting	

Integration Requirements

Describe any integration requirements with new or existing systems.
(enter description)

Impact

Describe impact to agency in the following areas:

Item	**(enter description)**
Agency processes	
Agency staffing resources	
Agency existing systems	

Risk

Risk List

Identify risks and associated probability, impact, and mitigation/contingency. (add additional risks as is required)

ID (enter number)	Risk Statement (enter description)	Risk Probability (1-5)	Risk Impact (1-5)	Risk Rating	Risk Mitigation (describe)	Risk Contingency (describe)
				0		
				0		
				0		
				0		

Recovery Time and Point Objectives

Describe RTO and RPO below.

Item	(enter description)
RTO	
RPO	

Data Classification

Identify the data classification in accordance with the data and system security classification grid as specified in the Arkansas Data System Security Security Classification Standard (SS-70-001 http://www.dis.arkansas.gov/Websites/dis/images/SS-70-001_dataclass_standard.pdf).

(select item)

Regulatory or Compliance Provisions

Identify any Regulatory or Compliance standards to which data or use of the service is subject.

HIPPA	
FERPA	
IRS (Publication 1075)	
FIPS (encryption standard)	
FISMA	
HITECH	
PCI (Payment cards)	
CJIS	
SSA	
FTI	
	(enter description)
Other	

Vendor Management

	(enter description)
Describe any SLA requirements and methods for monitoring of vendor compliance with SLA requirements:	
Describe exit strategy in the event of service disruption or vendor failure:	

Cost of Ownership and ROI

Cloud versus On-Premise

Summarize the TCO of each option over a 5 year period.

	Cloud (enter amount)	**On-Premise (enter amount)**
Infrastructure Equipment Cost (Including maintenance, this should also include any costs specific to the use of Cloud based services):		
Service Subscription Costs (Including initial fees for startup, and ongoing Cloud service cost):		
Network Connectivity/Bandwidth (This should include any increases in network capacity for use of either Cloud or On-Premise platforms):		
Transaction costs or data transmission charges (This should include per transaction costs for either platform or anticipated egress charges for data out of the Cloud):		
Backup and Recovery Costs (This should include additional storage, software, or DRaaS costs):		
Implementation Costs (This should include dedicated services for startup, migration, data cleansing, contract management, etc.):		
On-going Labor (This should include direct support ongoing administration and support cost for the infrastructure or service, and any ongoing indirect costs such as vendor/contract management activities):		
Other Costs (enter description):	**Cloud (enter other costs)**	**On-premise (enter other costs)**
TOTAL	$ -	$ -

ROI

Describe any cost savings, direct revenue, strategic, or requirement compliance benefits of the initiative, including the anticipated timeframe until the returns are realized.