North Carolina Department of Cultural Resources

Division of Archives and Records

NORTH CAROLINA
DEPARTMENT OF
CULTURAL
RESOURCES
WWW.NCCULTURE.COM

Best Practices for Cloud Computing

Records Management Considerations

Version 1.0

August 2012

TABLE OF CONTENTS

NOTE:

This document is a topical overview intended to provide information to state and local governments about common cloud computing concerns with regards to their records. This is not a complete list of issues to consider before adopting cloud technologies. Depending on the unique needs and restrictions of your organization, other factors requiring evaluation and exploration will emerge. Seek assistance from an attorney and your agency's Information Technology (IT) department for legal advice and/or specific technical questions.

1. Introduction to Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as a "model for enabling 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."[1] At its core, cloud computing can be understood as the acquisition and sharing of computing resources in a way similar to traditional utilities. Typically, service is available on-demand and customers pay for the amount of service they use. This model usually refers to infrastructure usage rather than licensing. Those fees are negotiated separately. The growing popularity of cloud computing over the past few years is a by-product of the provisioning of IT services over the Internet. It provides access, typically through the Internet, to services traditionally provided and supported in-house.

Cloud computing uses several preexisting technologies such as high-speed Internet, clustering, client-server computing, and large geographically distributed data centers. Cloud computing is merely the collection of these services offered together as one package. While adoption by the government sector (federal, state, regional, and local) has progressed more slowly than the private sector, government entities are increasingly looking to the cloud to be part of the solution for a range of IT needs. "Hybrid IT" is an emerging pattern where a portion of one's IT services are deployed to a public cloud while core services are retained in-house. For agencies that conduct operations online, cloud computing allows employees to access content and services regardless of their location or preferred computing device. This mobility is one of many advantages offered by cloud technology. Other commonly cited benefits for using "the cloud" include lower IT operating costs, faster IT implementation, increased productivity, and enhanced security.

Essential characteristics of cloud computing include multi-tenancy, on-demand self-service, broad network access, pooling of resources across multiple users, elasticity to respond to increased demands, and measured service based on pay-per-use. In other words, the service offers scalability to meet increased or decreased demand without requiring additional investment in fixed cost

[1] Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing (Draft),* NIST, January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

infrastructure to the agency. The service provider is tasked with bearing the brunt of those costs and incorporates that structure into its business model. There are four service models for adopting cloud computing: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Data-as-a-Service (DaaS)

These models are often referred to as “cloud layers” because services are built on top of one another. IaaS is the foundation of all cloud services. PaaS builds upon IaaS. And SaaS builds upon PaaS. NIST describes the models as follows:

	Who Uses It?	**What Services are available?**	**Why Use it?**
DaaS	Business Users	Geographic, financial, and historical data necessary for customer business	To aid in business decisions
SaaS	Business Users	Email, Office Automation, CRM, Website Testing, Wiki, Blog, Virtual Desktop…	To complete business tasks
PaaS	Developers and Deployers	Service and application test, development, integration, and deployment	Create or deploy applications and services for users
IaaS	System Managers	Virtual machines, operating systems, message queues, networks, storage, CPU, and memory, backup services	Create platforms for service and application test, development, integration, and deployment

Figure 1: General Services Administration Cloud Service Models and Use Cases

- Infrastructure-as-a-Service (IaaS): The on-demand infrastructure, a combination of hosting, provisioning, hardware, and basic services, offered to a user to operate a cloud. The user does not manage the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications. Examples of cloud infrastructure include Amazon’s Elastic Cloud Compute© and RedHat’s Cloudforms®.

- Platform-as-a-Service (PaaS): The capability offered to users to deploy their own applications onto the cloud through the provider’s resources. The user does not manage or control the underlying infrastructure, but does maintain control over the deployed applications. Examples of platforms include Facebook©, Intuit©, Force.com®, Rackspace©, and Sharepoint®.

- Software-as-a-Service (Saas): Software applications are remotely owned or managed by the provider and are accessible to users through a client, typically the Internet. The user controls neither the underlying infrastructure nor applications. Examples of SaaS applications include web-based email, iCloud©, GoogleDocs™, Dropbox©, and Survey Monkey™.

2. Purpose

State agencies are required to adhere to the Statewide Information Security Manual, published by the Office of the State Chief Information Officer. State agencies must also consider Session Laws of North Carolina, SL 2011-39. §11(c), which mandates that "State agencies developing and implementing information technology projects/applications shall use the State infrastructure to host their projects."[2] However, an exception to this requirement may be granted if approved by either the State Chief Information Officer on the basis of technology requirements or by the Office of State Budget and Management based on cost savings. When vetting potential service providers, it is important to keep in mind the directive set forth in the manual that states "vendors of cloud computing services shall agree with all Statewide Information Security standards when the State utilizes such services".[3]

Finally, computer systems that are not part of the State of North Carolina computer system but require connectivity to the state network or to agency networks must conform to state and agency security standards. Local governments and agencies should consider both federal and state best practices with regard to cloud computing as they move forward with their implementation of cloud base solutions. When considering cloud technology it is important to realize that cloud technology is not an all or nothing endeavor. Your office may choose to use it for only part of their technology needs. You should evaluate and understand your agency's operational needs in order to determine if adopting all or part of a cloud-based solution is feasible. When considering cloud technology, determine what motivates the decision:

- An inability to provide in-house services?
- A need to reduce costs?
- A desire to access content anywhere regardless of location?
- A need to redirect resources from IT infrastructure towards other organizational needs?
- Do you need to consider more than one cloud vendor to meet your business needs?

Cloud applications can be used for a variety of purposes including collaboration, communication, storage, access, or delivery of content.

[2] *Session Laws of North Carolina* 2011-391 (HB 22).

[3] Office of the State Chief Information Officer, *Statewide Information Security Manual* 2011, 21. https://www.scio.nc.gov/Mission/InformationSecurityManual.aspx.

Records (any Word document, email, text, chat, calendar, database, Excel document, etc.) that are made or received in connection with public business are public records. Transactions of public business conducted through cloud-based services are also public records and must be managed in accordance with each record's retention and disposition schedule. This requires greater attention to an office's records retention procedures and consideration as to how records will be handled in the cloud. If the office is going to offer content through the cloud while also hosting the data in-house, records management may proceed as it traditionally would with locally managed data. However, if the records are managed exclusively in the cloud, careful consideration should be taken regarding the implications of cloud storage for records management. For example, if the contract with the cloud vendor expires or the service is no longer supported by the vendor, you will need to download those records as well as any corresponding metadata onto a local system. The transfer must maintain the integrity of the files and you must be able to assure that the files are transferred accurately and completely. The use of cloud applications for storage will shape concerns related to security and confidentiality, ownership, ease of data removal/portability, and disaster recovery.

Regardless of your agency's intended use for cloud technology, understanding user expectations and whether they are being met by the service provider is critical. Ultimately, your agency should understand the impact of those issues before investigating cloud services or software. As you consider incorporating cloud technologies into your IT platform, pay attention to the following areas as you assess cloud providers and the services they offer.

3. North Carolina State Agency-Specific Compliance Issues

All state agencies in North Carolina must adhere to the *Statewide Information Security Manual* (SISM) issued by the State Chief Information Officer (CIO).[4] Depending on the operations of the agency, additional standards and statutory requirements may apply, such as the Health Insurance Portability and Accountability Act (HIPAA). Agencies are also required to follow § 132-1.10, which states that any agency of the State or its political subdivisions, or any agent or employee of a government agency, that experiences a breach of personal information, as defined in Article 2A of Chapter 75 of the General Statutes, shall comply with the requirements of G.S. §75-65. From a records management standpoint, North Carolina law does not distinguish between records stored in the cloud and records stored on site. However, cloud technology presents new challenges and complicating factors for records retention that must be addressed. It is important to remember that records generated and retained in the cloud remain public records. They are subject to the records retention and disposition schedules and generally subject to public access.

[4] Office of the State Chief Information Officer, *Statewide Information Security Manual* 2011, https://www.scio.nc.gov/Mission/InformationSecurityManual.aspx.

G.S. §75-65 requires notice be given to those affected when there has been a breach following discovery or notification of the breach. The disclosure must be made without unreasonable delay, consistent with the legitimate needs of law enforcement and “consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.”

Any business that maintains or possesses records or data containing personal information of North Carolina residents, or conducts business in North Carolina that maintains or possesses records or data containing personal information not owned or licensed by the business **shall notify** the owner or licensee of the information of any security breach immediately following discovery. Thus, in the event of a security breach, both the government entity and cloud provider are responsible for disclosure to affected persons.

Additionally, state agencies should be mindful of Session Law 2012-142, §6A.9.(b), State Private Cloud. The law declares that “the creation of a secure and flexible State private cloud is in the best interest of the people of this state.”[5],

4. Understanding and Negotiating the Terms of the Service Level Agreement

Issues discussed in this paper are similar for both subscription-based cloud service and free cloud services. However, the default agreements for public cloud providers typically do not provide adequate safeguard measures for an individual organization’s security and privacy needs. Contact your IT department for more information regarding security requirements. The relationship between consumers and cloud computing providers is contractually governed by the Service Level Agreement (SLA). This serves as a covenant between the consumer and service provider of the expected level of service. It states specific parameters and minimum levels for all areas of service provided. The SLAs must be enforceable and address specific remedies that apply when the contract is not met adequately. Before signing an agreement, a thorough assessment and evaluation of the service provider and the lifecycle of the service should be conducted to determine if the service provider can meet the consumer’s needs. Not all terms of an SLA are negotiable. But negotiations should at a minimum address areas described in greater detail below.

5. Performance and Monitoring

A typical SLA outlines metrics such as uptime/reliability, throughput, and service response times to determine whether the provider is delivering the agreed-upon service. This requires some method for monitoring service as well as a common understanding of performance definitions. The SLA must clearly define the

[5] SL 2012-142, House Bill 950, An Act to Modify the Current Operations and Capital Improvements Appropriations Act of 2011 and For Other Purposes, §6A.9, a-f, accessed July 27, 2012.

metrics to ensure a mutual understanding of the obligations and expectations for both consumers and providers. To assess potential violations of the contract, the agency may want to specify a neutral third-party organization to monitor the performance of the provider. Otherwise the consumer is liable for any breaches that occur with loss of data or availability.

The role of the SLA is not limited to determining uptime and performance/monitoring. Other issues often covered include data preservation, data privacy, and security. As with any contract, you must understand the terminology and legal ramifications of the document. Confirm all desired business and legal requirements are met in writing. Ultimately the consumer is responsible for understanding how the provider will honor its contractual obligations. Additionally, in accordance with G.S. § 147-22.89, state agencies must "develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology."[6] In addition, executive branch state agencies are also subject to Executive Order 102-Continuity of Operations and Continuity of Government Planning. This executive order, issued in 2006, commands all executive state agencies to "prepare a Continuity of Operations and Continuity of Government Plan to ensure the State's ability to deliver essential services under any circumstance."[7] Records hosted by cloud providers are subject to both G.S. § 147-22.89 and E.O. No. 102 and need to be addressed and provisions made to ensure the data is accessible in a disaster.

- **Availability**: refers to operational performance and user access to the system. Uptime is the amount of time the system can be expected to run without interruption. More critical applications require an increased level of availability in the cloud. The agency must determine the level of reliability required to meet this need. Downtime is defined as failure to deliver the expected service. Two types of downtime must be considered when choosing a service provider: the amount of planned downtime and the frequency of unplanned downtime. Planned downtime includes any time planned for applications to be offline to perform system maintenance or enhancements such as system upgrades. Unplanned downtime occurs by hardware or software failure. When defining availability requirements consider the following:
  - What are the operational consequences if the cloud is down? Can you quantify the cost to your agency?
  - What do you consider a "reasonable" or acceptable amount of time to be down?
  - How might downtime affect user experience or perception of the agency if you are delivering content to your citizens via the cloud?
  - Levels of required availability will drive the costs of cloud computing. Be sure your requested availability is appropriate to the business need

[6] G.S. §147.33-89(a). Business continuity planning
[7] Easley, Michael. Office of the Governor, "Executive Order No. 201-Continuity of Operations and Continuity of Government Planning." Last modified June 2006. Accessed June 15, 2012.

as cost may increase dramatically if you demand 24/7 service or “hot” sites.

The SLA should establish any compensation paid by the service providers based on the number of hours the system or service is down. In addition to the amount of acceptable downtime specified in the SLA, it may also be helpful to look at the reliability of the underlying technology. Is the technology sufficient to provide the required amount of service? Does the cloud vendor have the capability of hosting your content at more than one site? Is it sufficient to address your needs for Continuity of Operations Plan (COOP) and disaster recovery? What provisions does the provider have in place in order to address shortcomings in the service?

- **Governance:** The use of cloud technologies requires an office to relinquish some control and oversight of data as well as the security of the data. While cloud computing is intended to simplify operations and reduce costs, it may require greater governance and oversight. Offices should develop organizational controls for cloud computing that align with in-house technology practices. One way to test a vendor’s services is to use it as a development or test environment. Your office should develop policies and best practices for implementing and testing services (i.e., comply with statewide standards). Additionally, your office should develop and deploy a comprehensive audit system or workflow process to ensure that data is stored, protected, and used in accordance with office practices.

- **Compliance**: Laws and regulations may complicate security and privacy for cloud computing adoption as specific data requirements applicable to your office must be followed regardless of where the data lives. Requirements pertaining to government or industry-related regulations, confidentiality, and privacy controls must be addressed by the service provider before you begin using their technology.

Other issues to examine include the process of controlling and granting access to the cloud and ensuring that data is protected. Ultimately, it is the responsibility of the office to ensure that legal and/or regulatory requirements are met. See the above section on “North Carolina specific issues” for more information. Additionally, the (IT cloud computing document) contains a comprehensive overview of security related concerns for cloud computing.

6. Service Interruptions

Despite claims for uninterrupted service, even major cloud providers such as Microsoft® and Amazon® can experience service outages. If your agency is using or plans to use cloud services, you need to protect yourself in the event of a service outage and to ensure business continuity. It is important to explore what can be done to prepare for possible interruptions and what backup measures are or should be in place in the event of an outage. Although the SLA establishes the expected uptime from the service provider, it is impossible to predict unexpected or prolonged service interruptions. In accordance with G.S. §147-22.89, offices should have a continuity of operations plan ready in the event of a service outage. If an office loses access to the data, all their operations hosted or managed in the cloud could come to a halt. This may prevent the office from providing services or information to their clients as well as create a legal liability for failing to provide these services.

A cloud-specific contingency plan should be developed and integrated with a preexisting Continuity of Operations Plan (COOP). The office should determine its operational needs, requirements for storage, classification of data, and determine acceptable risk levels for information held in the cloud. Any solution must meet the agency's particular operational needs by determining risks, requirements, and classifying data assets. Your office should examine how they intend to use cloud technology—as a storage site that mirrors locally hosted data, the sole storage entity for data, or as a collaboration tool while documents are being drafted. Things to consider while developing a COOP to address offsite data held in the cloud include:

- Identify what data is most critical for continuing operations.
- Identify data that contains sensitive or personally identifying information.
- Determine duration of data retention and how often it needs to be backed up.
- Determine how employees will communicate in the event that they lose access to email or data.
- Determine if it is feasible to use a third party provider to maintain an additional copy of the data. This could be crucial to data recovery.

Certain applications and data can withstand downtime without significant impact and work well for storage in the cloud. Items such as time-sensitive or critical data may be less suited for use or sole storage in the cloud and should be maintained locally. This includes mission-critical data of your organization that could create a security and/or legal risk if breached. Using cloud services does not need to be an "all or nothing" endeavor; your agency can put as much or as little data into the cloud as necessary to meet its business requirements.

While business continuity pertains to how an office would function in the event of some sort of interruption, disaster recovery focuses on the technology systems that support business functions and is a subset of business continuity.

When selecting a cloud service provider, pay close attention to the provider's disaster recovery plan and the specific details established in the SLA. It is important for your office to:

- Understand what constitutes a disaster
- Know who can declare a disaster
- Be aware of what measures are in place to minimize impact to operations
- Know the Recovery Point Objective. This includes how current the data must be and how much data loss the agency can tolerate

- Know the Recovery Time Objective—how quickly the agency needs to be operational after any disaster

All potential providers should detail their service interruption strategies, such as a hybrid in-house/cloud system, disk backups, or off-site data replication. These are important to ensure minimal losses in the event of a disaster.

Testing is a critical element of a disaster recovery plan. This enables potential problems to be identified and addressed before they occur. Testing also provides an opportunity to verify projected recovery times and data integrity in advance of an incident. Continuity of Operation Plans (COOP) should be viewed as "living" documents that must regularly be updated to reflect the current state of system requirements, disaster recovery procedures, organizational structure, and policies of the agency. Your disaster recovery process and procedures should be documented and available in multiple locations.

For more information on developing a disaster recovery plan, the NIST *Contingency Planning Guide for Federal Information Systems* and Michigan's Government Cloud Protection Initiative offer suggestions specifically tailored to government agencies. The Council of State Archivists developed records-related emergency training for state and local governments through the Intergovernmental Preparedness for Essential Records Program (IPER). This information, which includes material related specifically to North Carolina, is available upon request.[8]

7. Costs

Much of the cloud's appeal stems from the claim that it significantly reduces IT costs, allowing your agency to shift more resources to core functions. While this is the case for many organizations, it is not necessarily always true. Often cloud services contain hidden costs. Most cloud services are based on a subscription model in which the organization pays a subscription fee to the service provider, minimizing upfront costs. However, unanticipated fees may complicate forecasting true service costs. Offices must understand and determine the total cost of operations and fees that may be charged before signing an agreement.

A Return on Investment (ROI) analysis will increase understanding of the true costs associated with adopting cloud services. At minimum, a comprehensive ROI should address hardware savings and possible infrastructure costs, personnel savings associated with reduced IT support, increased organizational efficiency, as well as monthly service provider subscription costs. Beyond the subscription fees, there are often additional charges from the service provider that are often overlooked in the ROI assessment. These include but may not be limited to:

[8] IPER Course Material, *Resources and Assistance in NORTH CAROLINA for topics covered in the IPER courses*, http://rc.statearchivists.org/Resource-Center/State/NC/IPER-Course-Material.aspx.

- **Migration and download fees**: Service providers often charge for data transfers in and out of the cloud based on the volume of data transferred. Be mindful of upload and download rates. And ask your vendor if rates will vary from year to year or remain constant for the duration of the contract.
- **Software**: Some cloud services may also require you to purchase the software in order to manage your data. Often, vendors sell different configurations of software or “seat licenses.” Typically, each person using the software or system requires a license to do so. This can be quite expensive or may limit your use of the product and create inefficiency if only a handful of people can use it. Another popular configuration is “concurrent” licenses. In this model, the buyer purchases a limited number of licenses but those licenses can be shared across several people. When talking with vendors, be sure to ask how you will manage the data in their offering and if that is part of the cost or if that is additional.
- **Integrating applications from multiple vendors**: To use cloud applications with in-house applications you may need to pay for integration. Costs depend on the extent of integration. Integration can be performed by the service provider and typically is an added expense, separate from the initial subscription.
- **Bandwidth** Efficient use of cloud services depends on a fast and reliable network connection. The North Carolina Office of Information Technology Services offers a Wide Area Network (WAN) to any authorized government entity in the state. WAN costs are calculated by use. Larger data will need a bigger “pipe” to get through. Is the existing level of bandwidth used by your agency sufficient to meet your specific cloud computing requirements? If you require greater bandwidth usage in order to use your cloud technology that may require an upgrade, resulting in increased costs.. Be sure to understand the costs before you proceed.
- **Backups**. IT best practices typically include a provision for backups of data. As you consider the “cloud,” consider the level of responsibility for the service provider to maintain data backups. Is this service included in the core cost of the agreement? Or is it a feature that must be purchased separately? Determine if there is an initial cost for implementing a backup system and monthly fees for the service.

8. Security and Privacy

Privacy and security issues must be adequately addressed before adopting cloud services. An understanding of your office’s security and privacy requirements will be important in developing a compliant solution. Assessing the terms of service in the SLA is important for deciding if the service will adequately meet your office’s needs. As you begin to examine security and privacy requirements, it will be important to consult your IT department.

9. Removing Data from the Cloud and Avoiding Vendor Lock-in

It is important to know what will happen to your data upon termination of the contract:

- How can it be retrieved?
- In which form and format?
- If you enhance your data in the cloud, will you also get a copy of that data as well? Or is the agreement solely for the original data?
- Will the service provider be required to keep the data on its systems during a transition period?

A key element to consider is whether or not there will be a charge to extract data from the cloud. Providers typically charge per gigabyte for transferring data in and out of the cloud. So understanding the overall cost before committing to a vendor is important.

As the agency negotiates the Service Level Agreement with a service provider, take the time to clarify your agency's ownership rights of all data that will be stored in the cloud. The SLA should develop provisions for returning or destroying data as directed by the agency, as well as a timeframe for completion. For data that will be returned to the office, protocols for how data is formatted and secured are important to establish. Due diligence and well-informed decisions are the best preventions to lock-in. Negotiating an SLA that clearly articulates the level of portability expected from a provider is crucial, as well as an understanding of who owns the platform, data, and tools. One best practice is to conduct a pilot of both putting data in and extracting data from the cloud. In doing so, you can determine how your agency will best accomplish these tasks.

A similar issue of concern is cloud lock-in. In this situation, the agency is stuck, or locked-in, with their current provider because of the complications and costs of switching to a new vendor. The use of a cloud solution could potentially require buying into the specific protocols, standards, and tools of the provider. This could make future migration costly and difficult. There are three types of cloud lock-in:

- **Data Lock-in:** Can the agency remove its data and if so in what form? Is data returned from the cloud in the same format in which it was uploaded? Can you get everything exported in total or only certain slices or views? What is the cost to extract this data? Is it included or is it a separate fee? Does the data extraction include the log files and analytics? In what format(s) is the data available—proprietary to the software or open?

- **Platform Lock-in:** The platforms built to provide applications and services are typically proprietary and can make migration between providers with different platforms cost prohibitive. Does the provider use a proprietary programming language, data model, or run time environment?

- **Tool Lock-in:** Cloud providers offer a variety of tools to customers. To avoid tool lock-in, you need to ensure a cloud provider's provisioning and monitoring tools are "compatible" with different kinds of infrastructure. Would the use of third party web services from the provider require you to find or build alternatives?

10. E-Discovery Guidelines

Electronic Discovery ("E-Discovery") is the legal process of gathering electronic information from each of the parties in a lawsuit.[9] When responding to E-Discovery requests, employees should consult the attorney for his or her state agency or local government. E-Discovery in the cloud presents a new set of challenges as ownership and control, cost, destruction of data, and jurisdictional issues must be considered. Courts generally do not distinguish between *data in possession* and *data under control* for purposes of discovery. In 2011, the North Carolina Rules of Civil Procedure (NCRCP) was amended to address issues related to E-Discovery. It now states that electronically stored information (ESI) and "reasonably accessible" metadata are subject to discovery in civil litigation.[10]

- **Data Ownership and Control:** Data sourced to a cloud system should remain the legal property of the agency. NCRCP 34 establishes the scope of the request as being in the "possession, custody or control of the party upon whom the request is served." While the Service Level Agreement (SLA) should clearly articulate the agency's ownership of data, it should also make clear that if the provider is subpoenaed for documents held in the cloud, the provider may be obligated to provide data based on its possession and custody. Conversely, the agency maintains its responsibility to preserve and produce data that is not in the party's "possession" or "custody," but nonetheless is within its "control."[11]

- **Costs:** The provider may have either enhanced or limited technological capabilities that may impact the cost of preservation and access. For enhanced technologies, a more in-depth search may be required because the data can be searched at little or no cost.

- **Destruction of Data:** Records retention and disposition schedules serve to cut costs for discovery and storage, as well as reduce risk. These schedules allow agencies and offices to destroy records after certain time thresholds have been met. By destroying records in a timely fashion, agencies and offices can save considerable time and money during E-Discovery. However, providers are not necessarily bound to adhere to the agency's retention policy and could inadvertently expose the agency to greater litigation risk by retaining data longer than the records retention schedule proscribes. Conversely, data intended for permanent or long-term retention might be accidentally erased or overwritten by the provider's server, thereby breaking public records law. The SLA should address the provider's obligations, if any, to uphold the agency's retention

[9] For more information, see the Department of Cultural Resources guide "Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition", November 2010 http://www.records.ncdcr.gov/erecords/default.htm.

[10] Kara Millonzi, "Metadata, E-Discovery, and E-Public Records in North Carolina," September 15, 2011 http://sogweb.sog.unc.edu/blogs/localgovt/?p=5432.

[11] David D. Cross and Emily Kuwahara, *E-Discovery and Cloud Computing: Control of ESI in the Cloud*, EDDE Journal 1, (Spring 2010).

policy, as well as measures for recovering data or providing compensation in the case of permanent data loss.

- **Jurisdictional Issues:** The use of cloud services may increase litigation exposure by providing additional areas for jurisdictional determinations. It is important to select a provider who stores data only in jurisdictions where the agency is prepared to defend litigation as cloud servers may be located in other states, federal circuits, or even another country.

In addition to the areas outlined above, the SLA should specify the provider's obligations should the agency become the subject of a subpoena or other legal or governmental request for access. If possible, negotiate with the provider to establish a policy of notification to the agency as soon as the provider receives any request, before they provide access to any data, and to cooperate with the agency's efforts to manage the release of data. It will be extremely important to consult your legal department for assistance with specific questions or advice.

11. Summary

Despite complicated issues related to cloud computing, with due diligence and foresight, your office can prepare for any challenges. First, understand the obligations and guarantees established in the Service Level Agreement. Second, be prepare to negotiate with a service provider to ensure that the contract fulfills the legal and operational requirements of your agency. This requires knowing the specific requirements and needs of the agency as well as how adoption of cloud solutions can adequately meet these needs. Finally, discuss any decision to use cloud services with other groups in the agency, particularly attorneys and IT, to ensure that legal and technical requirements are met.

Public records produced in the transaction of state business are subject to several North Carolina statutes and executive orders:

- G.S. §132–the Public Records Law,
- G.S. §121–the Archives and History Act.
- G.S. §147.33-89(a).–Business continuity planning
- NCAC 04M.0101–Statement of Purpose of Archives and Records Section
- Executive Order No. 201, Michael Easley, Office of the Governor, "Executive Order No. 201, Continuity of Operations and Continuity of Government Planning."
- Executive Order No. 18, Bev Perdue, Email Retention and Archiving Policy

As such, regardless of where public records physically reside for storage or access, they are subject to the same criteria. If your office is considering moving records into the cloud, externally hosted infrastructure, this document provides guidance on issues impacted by such a decision. As records creators and custodians, state and local employees must ensure that their records are protected if confidential and accessible in the event of litigation or a public records request.

Appendix A: Definitions

Continuity of Operations Plan (COOP): Provisions for identifying and protecting records, along with implementing a vital records program needed to support the office's essential functions during an emergency situation and to protect the legal and financial rights of citizens.

Federation: Ability to bring together services from various cloud vendors to provide a solution.

Interoperability: Ability for different clouds to talk to each other.

Lock-in: When there is significant cost to switch cloud vendors.

Migration: Act of moving from one service provider/vendor to another

Portability: Ability to move application, data, tools from one cloud to another.

Private Cloud: Services offered over the Internet or over a private internal network only to select users; not available to the general public.

Public Cloud: Services offered over the Internet and available to anyone willing to purchase the service.

Recovery Point Objective (RPO): How current the agency's data must be and how much data loss the agency can tolerate.

Recovery Time Objective (RTO): How quickly the agency needs to be operational after any disaster.

Reliability: Cloud reliability refers to whether the cloud resources perform consistently within their specifications.

Return on Investment: an accounting formula used to obtain an actual or perceived future value of an expense or investment.[12]

Scalability: Ability of the cloud infrastructure to expand and contract to meet shifting user demand. Also referred to as Elasticity.

[12] Webopedia, "Webopedia: Everything You Need to Know is Right Here." Accessed July 5, 2012. http://www.webopedia.com/TERM/R/ROI.html.

Bibliography

Council of State Archivists. *Resources and Assistance in North Carolina for topics covered in the IPER courses*. http://rc.statearchivists.org/Resource-Center/State/NC/IPER-Course-Material.aspx

Cross, David D. and Emily Kuwahara,. *E-Discovery and Cloud Computing: Control of ESI in the Cloud*. EDDE Journal, Vol. 1 No. 2, (Spring 2010).

Curtis, Wendy Butler, et. al, *Cloud Computing: eDiscovery Issues and Other Risk,* Orrick eDiscovery Alerts, (June 2010).

GSA. *Federal Cloud Computing Training*. Info.Apps.Gov, Document Library. August 2009. http://info.apps.gov/content/document-library

Minnesota Historical Society*. Preserving State Government Digital Information*. August 2011. http://www.mnhs.org/ndiipp.

National Institute of Standards and Technology (NIST) Definition of Cloud Computing (Draft). NIST. January 2011. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

National Institute of Standards and Technology (NIST). *NIST Special Publication 800-34, Rev.1, Contingency Planning Guide for Federal Information Systems*. NIST. June 2008. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=905266

National Institute of Standards and Technology (NIST). *Draft Cloud Computing Synopsis and Recommendations*. May 2011. http:/*/csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf*

National Institute of Standards and Technology (NIST). *Guidelines on Security and Privacy in Public Cloud Computing*. January 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

National Institute of Standards and Technology (NIST). *US Government Cloud Computing Technology Roadmap Volume II*, Release 1 (Draft). November 2011.

State of North Carolina Office of the State Chief Information Officer. *Statewide Information Security Manual.* June 2011*.* https://www.scio.nc.gov/Mission/InformationSecurityManual.aspx

The Sedona Conference. *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document*

Production, 2nd ed., 2007.

Software and Information Industry Association (SIIA). *Guide to Cloud Computing for Policymakers.* 2011. http://www.siia.com/index.php?option=com_content&view=article&id=792:guide-to-cloud-computing-for-policymakers&catid=66:public-policy-overview&Itemid=851

2010 NASCIO Recognition Award Nomination*. The Government Cloud Protection Program: Disaster Recovery Services Transformed for the Perfect Storm*, 2010. http://www.michigan.gov/dmb/0,4568,7-150-9131-239407--,00.html.

Yasin, Rutrell. *What's missing from the cloud? An exit strategy.* GCN: Government Computer News. May 23, 2011. http://gcn.com/articles/2011/05/23/cloud-survey-no-exit-strategy.aspx

Trappler, Thomas J. *If It's in the Cloud, Get It on Paper: Cloud Computing Contract Issues*. Educause Quarterly Magazine, 33. 2010.