Cloud Computing:
Implications and Guidelines for Records Management in Kentucky State Government

(Version 1.0 August 2012)

Many information technology (IT) departments and resource allocators are considering implementing cloud computing services, also known as distributive computing. Two reasons frequently cited for using cloud computing services are potential cost savings brought about by economies of scale, and the ability to rapidly deploy new applications and services. Cloud computing has the potential to have a substantial impact on archives and records management in Kentucky government. This document examines some of the possible implications for recordkeeping in cloud computing and related technologies.[1]

Definition and Understandings

Cloud computing services often provide common business applications (email, document creation, etc.) online that are accessible from a web browser, while the software and data are stored on the service provider's servers. The Kentucky Enterprise Architecture and Standards Committee (EASC) defines cloud computing as "a style of computing in which massively scalable IT-enabled capabilities are delivered as a service to multiple customers using Internet Technology."[2] **The EASC requires all agencies considering the use of cloud computing applications to submit an exception request to the committee.**

One concern with the term, "cloud computing," is that it is too often used without referring to the established governmental definition. According to some, cloud computing is not so much a definition of a single term as a trend in service delivery. "It's the movement of application services onto the Internet and the increased use of the Internet to access a variety of services traditionally originating from within a company's data center."[3] By contrast, the national standard for cloud computing is established by the National Information Systems Task Force (NISTF).[4] If your agency, or an agency for which you provide services, is considering implementation of cloud computing services, it is very important to ensure that all parties involved – including the potential vendors of the cloud solutions – have a shared understanding of the exact terms of the proposal for the services. From a records management and archives point of view, it is difficult to identify the recordkeeping implications of implementing a cloud computing environment without having a clear understanding of the exact nature of the cloud computing proposal. Also, the evaluation of a cloud computing environment must consider Kentucky laws related to open records, records management, and auditing.

What are the Issues in Cloud Computing?

Given the many possible ways an organization could use cloud computing services, all stakeholders must be involved in the decision-making process. Archivists, auditors, legal staff, and records managers should be among those stakeholders. In fact, many areas of concern for records managers and archivists could serve as the basis for reaching consensus among all of the stakeholders regarding the use of cloud computing services within the organization. Standard 2050 of the Kentucky Enterprise Architecture and Standards identify the following issues with cloud computing:

> "One of the driving forces behind the utilization of "the cloud" is an expectation of significant cost savings as opposed to a closed source or vendor-owned software solution. However, cloud computing currently lacks security and privacy guarantees necessary to support much of government's internal functions. Some concerns that are not fully defined include, but are not limited to: the physical location of the data (U.S. vs. overseas), sanitation of equipment prior to disposal, security vulnerabilities of the applications themselves, security vulnerabilities of data in transit, and audit logging and regulatory compliance become very prohibitively complex. **A lack of standards within the industry, at the present time, creates unacceptable levels of risks to the overall security of the Commonwealth's data."**

Listed below are a few issues for archivists and records managers to consider if their organization is considering using cloud computing services. This is by no means an exhaustive list.

Scope – What organizational information will be stored, processed, and accessed through the cloud? Will restricted data (personally identifiable information, law enforcement information, exceptions to the Open Records Act, etc.) be stored, processed, and/or accessed through the cloud?

Retention – Cloud computing vendors often create multiple copies of the data they store for an organization on geographically-dispersed storage media to ensure that data is not lost and is continually available to end-users. Record keepers should have a clear understanding of the methods used by the vendor to ensure the destruction of all copies of records that have reached the end of their scheduled retention period.

Preservation – For long-term or permanent records, the cloud computing services should prove a means of integrity checking and/or comparison of multiple copies stored on/off the cloud. Although cloud computing may provide partial solutions to complex preservation issues, these are beyond the scope of this document. Please consult the Kentucky Department for Libraries and Archives for strategies for long-term preservation**.**

Location – Cloud computing is often implemented in such a way that end-users are not aware of the location of their stored information or where it is processed. Some cloud computing service providers allow users to place broad limits on where data will be stored (e.g., in the continental United States, in a particular state, etc.) If your organization is contemplating storing data with jurisdictional boundaries in a cloud, it is important to establish location as a requirement prior to procuring services or negotiating contracts with a vendor.

Legal/Policy Compliance – "The ability of cloud computing services, especially public/community cloud computing services – to comply with the regulations, laws, and policies that govern the management of an organization's information, are often cited as one of the most significant barriers to wide-spread adoption of cloud computing by government entities and highly-regulated organizations."[5] Cloud computing services should be required to comply with all laws, regulations, and policies.

E-Discovery – Your agency may be subject to E-Discovery, which may require you to locate relevant information quickly. Records in litigation must be placed on hold and not be destroyed under existing records retention schedules until the litigation is completed. Methods for ensuring compliance with E-Discovery orders and other litigation-related actions relative to information stored in a cloud should be discussed with potential cloud computing service providers.

Interoperability – Because information stored in many information systems must be maintained and accessible long after the system has become obsolete, consider an exit strategy any time the organization considers the deployment of new information technology – including cloud computing services. Prior to using a cloud computing service, ensure that your information is accessible and not contained within a proprietary system that requires considerable expense or effort to remove and transfer the data.

Security – There is current debate in the IT community as to whether cloud computing services provide more or less security than "traditional" IT infrastructure. Security typically improves due to centralization of data, increased security focused resources, increased ability to patch and upgrade, increased ability to monitor, increased ability to encrypt, and many other reasons. There are concerns, however, about loss of control over certain sensitive data once it is stored in a cloud. When designed at the beginning, security of cloud architecture was significantly higher than non-cloud approaches. Enterprises requiring enhanced security should consider private clouds rather than public clouds. Records processed or stored in the cloud must comply with applicable COT, EASC and agency security policies and standards.

Community Cloud – Some government organizations are exploring options for implementing consortium type clouds for similar organizations that have like security, legal, privacy, etc. requirements. At least one major vendor of cloud

computing services has announced that it will provide a government cloud with a separate infrastructure just for government agencies.

Audits – Government cloud computing services should be mindful of the requirements of current auditing practices. The American Institute of Certified Public Accountants guide, "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC-2)*" provides the latest procedures followed by the Kentucky Auditor of Public Accounts.[6] Vendors providing cloud services should be audited annually following applicable audit standards with audits and management letters made available to its clients.

How can Agencies Meet Their Records Management Responsibilities?

State and local government agencies are required to manage their records through records retention schedules according to Kentucky Revised Statutes (KRS) 171.410-740 and Kentucky Administrative Regulations (KAR) promulgated through the General Assembly by the Kentucky Department for Libraries and Archives (KDLA). Regardless of which cloud computing service and deployment models are adopted, agencies are still required to comply with these statutes and regulations. Variations among these models, however, will affect how and by whom (agency/contractor) records management activities can be performed.

The following are guidelines for creating standards and policies for managing an agency's records created, used, or stored in cloud computing environments:

a. Include the agency records management officer and/or staff in the planning, development, deployment, and use of cloud computing solutions.
b. Define which copy of records will be declared the agency's record copy and manage these in accordance with the state or local government records retention schedules. Remember, the value of records in the cloud may be greater than the value of any other set because of indexing or other reasons. In such instances, this added value may require designation of the copies as records.
c. Include instructions for determining if state and local government records in a cloud environment are covered under an existing records retention schedule.
d. Include instructions on how all records will be captured, managed, retained, made available to authorized users, and records retention schedules applied.
e. Include instructions on conducting a records analysis, and developing and submitting records retention schedules to KDLA for unscheduled records in a cloud environment. These instructions should include scheduling system documentation, metadata, and related records.
f. Include instructions to periodically test transfers of state and local government records to other environments, including agency servers, to ensure the records remain portable.
g. Include instructions on how data will be migrated to new formats, operating systems, etc., to ensure records are readable throughout their lifecycle. Include

in your migration plan provisions for transferring permanent records from the cloud to KDLA.

h. Resolve portability and accessibility issues through good records management policies and other data governance practices. Data governance typically addresses interoperability of computing systems, portability of data (the ability to move from one system to another), and information security and access. Such policies by themselves, however, will not address an agency's compliance with KRS 171.410-740 and KDLA administrative regulations.

What is an Agency's Responsibility When Dealing with Contractors?

Ultimately, Kentucky government agencies maintain responsibility for managing their records whether these records are in a cloud computing environment or under an agency's physical custody. When dealing with a vendor, an agency must include a records management clause in any contract or similar agreement. At a minimum, a records management clause ensures that state and local government agencies and the vendor are aware of their statutory records management responsibilities.

The following is a general clause that an agency can modify to fit the planned type of service and specific agency records management needs:

> *Use of contractor's site and services may require management of state and local government records. If the contractor holds state and local records, the contractor must manage state and local records in accordance with all applicable records management laws and regulations, including but not limited to KRS 171.*410-740 *and administrative regulations of the Kentucky Department for Libraries and Archives (KDLA), as well as adherence to the Open Records Law and the regulations established by the Auditor of Public Accounts. Managing the records includes, but is not limited to; secure storage, retrievability, and proper disposition of all state and local records including transfer of permanently valuable records to KDLA in a format and manner acceptable to KDLA at the time of transfer. The agency also remains responsible under the laws and regulations cited above for ensuring that applicable records management laws and regulations are complied with through the life and termination of the contract.*

If an agency receives approval to join a private or community cloud, it must still meet records management and other regulatory responsibilities. Agencies may describe these responsibilities in agreements among the participating offices or agencies. If a cloud computing provider ceases to provide services, an agency must continue to meet its records management obligations, so agencies should plan for this contingency.

Conclusion

Many analysts agree that it is not a matter of if, but when, cloud computing services will be widely used by governments. Cloud computing has already been adopted by a few Kentucky government agencies, following the EASC's exceptions request process. If an agency contemplates deploying cloud computing services, the issues listed in this document need to be addressed in the initial system assessment. Agencies must also submit a cloud computing exception request for review by the Kentucky Enterprise Architecture and Standards Committee (EASC). Cloud computing services will continue to evolve over the near term, and new developments will need to be monitored. Because of the complex nature of both the technology and policy implications of cloud computing, it is important for archivists, auditors, records managers, and the legal community to work with other stakeholders in addressing these developments.

---

[1] These guidelines are based on Conrad, Mark. "Distributed Computing – Cloud Computing and Other Buzzwords: Implications for Archivists and Records Managers." NAGARA Crossroads 2009-3. http://www.nagara.org/displaycommon.cfm?an=1&subarticlenbr=79

[2] Enterprise Architecture and Standards, 2050 Cloud Computing. https://gotsource.ky.gov/docushare/dsweb/Get/Document-301104/

[3] Creeger, Mache. "CTO Roundtable; Cloud Computing," Communications of the ACM 52, No. 8(2009); 56, 50.

[4] Mell, Peter and Tim Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology (NIST SP - 800-145); September 28, 2011; pages 1-2. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909616

[5] Tucci, Linda. "Addressing Compliance Requirements in Cloud Computing Contracts." Search/CIO.com, June 11, 2009.

[6] AICPA. "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC-2)." http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0128210/PC-0128210.jsp.