JTC Resource Bulletin

Cloud Computing

Version 1.0
Adopted December 5, 2014

Abstract

Properly deployed cloud services offer a variety of potential benefits that can improve the efficiency and effectiveness of records and information management in the judiciary. It is important to understand cloud computing service models, deployment options, security risks, and implementation challenges when considering cloud computing.

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).

JTC Mission:
To improve the administration of justice through technology

Joint Technology Committee:

COSCA Appointments

David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Gerald A. Marroney
Colorado Administrative Office of the Courts

Robin Sweet
Nevada Administrative Office of the Courts

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

Ex-officio Appointments

John Greacen
Forum on the Advancement of Court Technology

NACM Appointments

Kevin Bowling (Co-Chair)
Michigan 20th Judicial Circuit Court

Paul DeLosh
Supreme Court of Virginia

Yolanda Lewis
Superior Court of Fulton County, Georgia

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Craig Burlingame
Massachusetts Trial Court

NCSC Staff

Paul Embley
Jim Harris
Ilonka Dazevedo

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	12/5/2014	JTC	Release document

Contents

Introduction

Whether we realize it or not most of us already depend on cloud computing in our daily lives. Web-based e-mail services like Hotmail, Yahoo! Mail or Gmail are the most common examples. Drop Box and other file storage services allow us to maintain digital materials such as documents, photos and recordings where they are easily accessible on line for sharing and use. Social media as well, rely on cloud services. Bottom line is, if the software and storage you access don’t exist on your computer, it's on the service's computer cloud.

As a business application the implementation of cloud computing by government agencies has generally lagged behind the private sector. However, this is changing. In 2010, the U.S. government took a significant step towards promoting the use of cloud solutions by issuing a cloud-first mandate and identifying related funding. The mandate directed federal agencies to adopt cloud computing in some capacity, and provided information on how to select cloud services. The National Archives and Records Administration published best practices for cloud system management of email[1] in September of 2014, following the migration of 3,000 of its email users to the cloud.[2]

Understanding how cloud computing works and the variety of services and options that are available under this concept is an increasingly important part of managing the core competency of information technology management.

What is Cloud Computing?

The National Institute of Standards and Technology (NIST) has been designated to develop standards and guidelines for the Federal cloud computing.[3] From a technical point of view, 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

[1] "Bulletin 2014-06 - Guidance on Managing Email." National Archives and Records Administration, 15 Sept. 2014. Web. 07 Nov. 2014.

[2] ARMA International. "U.S. Agencies Embrace the Cloud." *Information Management* 48.3 (2014): 19. Web. 7 Nov. 2014.

[3] "NARA Bulletin 2010-05 - Guidance on Managing Records in Cloud Computing Environments" National Archives and Records Administration. National Archives and Records Administration, 08 Sept. 2010. Web. 07 Nov. 2014.

and released with minimal management effort or service provider interaction."[4] This definition continues to evolve as the industry matures.

The NIST standards also identify the primary characteristics that are associated with cloud computing:

> ***On-demand self-service.*** Computing services such as server time and network storage are more scalable and can be used as needed without human interaction with each service's provider. This “pay-as-you-go” approach is one of the major appeals of cloud services.
>
> ***Broad network access.*** Capabilities can be provided over the network and accessed through a browser or via apps installed on a mobile phone, tablet, laptop, or workstation.
>
> ***Resource pooling.*** Computing resources can be pooled under a multi-tenant model. Users with different needs will have appropriate physical and virtual resources available based on individual consumer need. These include storage, processing, memory, and network bandwidth. Customers may not have knowledge or control over the exact location of the services, though they may be able to specify location at a higher level (country, state, datacenter) as part of a services agreement.
>
> ***Collaboration.*** Cloud applications by their nature allow for much greater collaboration between users who are able to access information and services through the Internet from computers, tablets and smartphones.
>
> ***Rapid elasticity.*** Resources and capabilities can be readily adjusted, either up or down, than would be the case in a local datacenter. In some cases, adjustments can be provided automatically without customer intervention.
>
> ***Measured Service.*** Cloud systems have the capability to automatically control and optimize resource use by metering services appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

[4] Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing." *Cloud Computing*. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Sept. 2011. Web. 07 Nov. 2014.

The technology that makes cloud computing possible is the Internet, which allows real-time access to systems and information. Properly deployed cloud services offer a variety of potential benefits to government agencies, including the courts. In theory, an organization could operate completely within a cloud environment without the usual IT infrastructure and staff that currently exist.[5] While this may not be the ideal model for today's courts, there are still opportunities provided by this technology that have the potential to improve the efficiency and effectiveness of records and information management in the judiciary. As courts consider cloud computing options it's important to understand the various service models for cloud computing services.

Cloud Computing Service Models

Cloud computing can include a variety of services. There are three service models typically available from cloud services providers: Software, Platform, and Infrastructure.

Software as a Service (SaaS)

This is perhaps the most well-known and common type of cloud service. SaaS is the ability to provide access to a software application from a single point to multiple users. The service provided to the consumer is the ability to use the application on the provider's infrastructure. Software applications are accessible to clients via their computing devices through a thin client interface such as a web browser. Under this model, users give up control over the underlying infrastructure such as servers, operating systems, and storage.

One benefit of this service model is that it reduces the local effort required to manage applications for each individual user because the software exists in one location (the cloud) and not on each user's device. This approach does, however, limit the ability to customize applications to meet individual user needs. When a cloud application is shared by numerous user groups, system performance may vary due to system demand. A SaaS solution is therefore best for a system that needs minimal customization for users.

Platform as a Service (PaaS)

Instead of providing a single application approach, PaaS solutions offer customized system and application platforms. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported

[5] Porter-Roth, Bud. "Toolkit: Cloud Content Management." *Toolkit: Cloud Content Management*. Association for Information and Image Management, 2012. Web. 16 Dec. 2014.

by the provider. PaaS solutions may take the form of a standardized operating system platform and are often used for application development or customized hosting. In this model, users do not manage or control the underlying cloud infrastructure (network, servers, operating systems, storage). Users do retain control over the deployed applications and their customization to the user environment.

Infrastructure as a Service (IaaS)

Cloud-based infrastructure services meet the needs of organizations that are growing and need additional processing and storage capacity, or where processing and storage needs are variable and difficult to predict. IaaS solutions provide the physical infrastructure for organizations to deploy and run the operating systems and applications of their choice. Users do not manage or control the cloud infrastructure, but do retain control over the operating systems and applications, as well as some components such as firewalls. The advantage of IaaS is that an organization can more easily adjust to changing needs for storage and processing without making substantial investments in new equipment and personnel.

The primary benefits of all of these approaches are the flexibility and typically low cost of entry. Depending upon user needs and other considerations, cloud computing services are typically deployed using one of the following four cloud environments:

Public cloud. Public clouds are the most visible type of service model. Offerings such as Amazon Web Services and Google Apps are examples of high-profile public cloud offerings. A public cloud is essentially infrastructure that is available to the general public or a large industry group, but owned and managed by a cloud vendor. Public clouds may be customized to meet the needs of specific industries or organizations.

Private cloud. Private clouds are similar to public clouds except that the cloud infrastructure is operated solely for an organization. A private cloud may be managed by the organization or a third party, and may exist on or off premises. The principle characteristics that differentiate a private cloud from traditional information infrastructure are the elasticity and measured resource utilization offered by the cloud services model.

A variation of the public cloud that has gained the attention of agencies that are concerned with security and regulatory requirements is the ***hosted private cloud***. A hosted private cloud can be viewed as an extension of a traditional data center that uses single-tenant servers and storage systems that are not shared between customers.[6]

Community cloud. For organizations that are concerned about security and compliance, a community cloud is often the preferred approach. The infrastructure of a community cloud is shared by several organizations and designed to support a specific community that has common requirements. Like the private cloud, a community cloud may be managed by the participating organizations or a contracted third party, and may exist on or off premises. The community cloud is a good option for government agencies which lack the resources and expertise to manage their own private cloud.

Hybrid cloud. The hybrid cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology. This approach is appealing to organizations that are subject to high levels of regulation and compliance, such as health care, by allowing some applications and data to reside inside the organization's security firewall while still taking advantage of the benefits of other cloud services. Cloud solutions clearly offer benefits in terms of agility, scalability, low cost of entry, and in many cases, longer-term costs savings. The variety of services and deployment models that cloud computing offers open the potential for a variety of approaches to managing court information ranging from the static preservation of archival records to a platform for the development and testing of new systems.

Architecture

At a very basic level, cloud computing architecture consists of a *front end,* which is the user, and the *back end*, which is the centralized storage and access to digital resources. The user is connected through a network, most often the Internet, to the back end or cloud portion of the system. The front end architecture includes the user's computer or other device, and the applications used to access the cloud system. User interfaces may vary depending on the type of service. Web-based e-mail programs often utilize Web browsers such as Chrome or Firefox. Others have interfaces which are unique to the system.

The back end or cloud side of the system includes computers, servers and data storage that are the universe or cloud of services. Almost any program imaginable could reside

[6] "Keys to Deploying a Hosted Private Cloud," MindSHIFT Technologies, n.d. Web. 07 Nov. 2014.

in the cloud environment, from complex and interactive application software to archival data. The system is generally administered by a central server which monitors traffic and usage demands to maintain consistent access and performance. This is accomplished through the use of special rules, or protocols, and specialized middleware software. The middleware supports communication between networked devices to balance load and usage. Through a technique called server virtualization, servers can be managed for peak performance efficiency.

Challenges

The decision to consider cloud computing solutions as part of a court's technology strategy raises a number of concerns. Some of these, such as vendor reliability and security, apply to information technology in general. Other issues, such as control and portability, are more unique to third party provisioning of cloud computing services.

Security

Security has been one of the most commonly expressed concerns by potential cloud computing customers. Major incidents involving unauthorized access to client data by public companies has created considerable concern about the ability of organizations to protect critical data. Concerns about security include both physical security and data security. Without knowing where the information resides, how is one assured that the information is protected from unauthorized access and that the facility is designed to withstand a natural or man-made disaster? Similarly, data security may be compromised by deliberate attack (hackers, viruses) or through unintentional loss or corruption. However, many argue that large cloud vendors have security protocols and conditions that exceed those of most local data shops. Experienced cloud providers often have greater resources available and substantial incentives to provide comprehensive security protection for their customers.

Control

The choice of a cloud computing model will have an impact on how records are created, used, and stored in cloud computing environments, as well as on the level of control that the court or its technology support personnel have over the cloud environment. For instance, in the case of IaaS and PaaS service models, it is more likely that records will be maintained outside the cloud, while in a SaaS service model, this responsibility would more likely be transferred to the contractor. These details must be addressed in the service contract.

Lifecycle Management

Cloud applications may lack records retention and disposition schedule capabilities, including the ability to transfer or permanently delete records pursuant to state or local retention schedules, and perform other records management functions such as legal holds and historical preservation of designated records. To utilize cloud services as an archival solution, you must identify and provide for these requirements. Records must be preserved in a manner that retains their functionality and integrity throughout the entire lifecycle. Links must also be maintained between the records and their metadata, including metadata associated with records which have been purged or destroyed. NARA cautions that many cloud architectures lack formal technical standards that are necessary for long term preservation of records.

Portability

Once records have been transferred to a cloud environment there may be problems regarding portability of the records in the event of the need to transfer the records back to the court's control or to that of another vendor or agency. Inadequate provision for portability standards and functionality may compromise the removal of records to meet disposition requirement or complicate their transition to another environment. The court should have a clear agreement with its provider regarding transfer and removal of records, and provisions for loss of business continuity by the vendor resulting from merger, bankruptcy, or other circumstances that prevent the vendor from providing the agreed-upon service. The costs of termination or transfer should be clearly understood.[7]

Vendor Reliability

Experience has shown how volatile the information technology business can be. The selection of a cloud provider should include an assessment of the provider's expertise in providing similar services, the vendor's size and financial stability, and prior reputation. Prior reputation may include the vendor's record of outages and their ability to recover from network, hardware, or other failures. The vendor's level of expertise and ability to provide timely support should also be considered.[8] The cloud services agreement should also include provisions for

[7] " Scaling Back in the Cloud-How to Extricate Your Data." *PC Today* 9.10 (2011): 28-29. Oct. 2011. *Internet Archive.* Web. 7 Nov. 2014.

[8] "Cloud Service Providers - 10 Key Considerations For Choosing The Right Ones." *PC Today* 11.4 (2013): 32-33. Apr. 2013. *Internet Archive*. Web. 7 Nov. 2014..

termination of the agreement and access to court data in the event of business termination or new ownership due to merger or acquisition of the cloud vendor.

Vendor Compliance

Courts that rely on third party vendors for records storage and maintenance, including cloud storage, have a duty to ensure that the vendor understands the security and access requirements for the information entrusted to the vendor’s care. Utilizing a cloud vendor can increase a court’s liability if the vendor is not compliant with court rules, statutes and federal regulations that govern information access, use, and security. For example, The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and related rules impose duties on “business associates” which may include a third party vendor. The court must ensure that the vendor provides the required administrative, physical and technical safeguards required by HIPAA rules if the vendor is managing court records that contain HIPAA-protected information.[9] The same applies to compliance with the FBI’s Criminal Justice Information Systems Security Policy for criminal records maintained and accessed through a third party-managed cloud.[10]

Ensuring vendor compliance with applicable laws may require more than a written assurance in the vendor agreement, and also include periodic audit reports and documentation of vendor safeguards. These conditions should be clearly stated in the vendor agreement.

All of these concerns point to the need for careful planning and documentation prior to implementation of a cloud solution. That planning must also address contingencies in the event of an outage, whether that outage originates with the cloud services vendor, your internet service provider, or within your building.

An important element of any relationship with a cloud services vendor is a service level agreement, or SLA. An SLA is a document that outlines the services to be provided, security and backups, pricing, levels and standards of service, and consequences for failure to deliver the agreed-upon service level. Any proposed SLA should be carefully reviewed and negotiated to ensure that the provider can meet (or exceed) the specific

[9] Shwayri, Rebecca N., J.D. "Balancing the Risks and Rewards of Cloud-based Healthcare Information." *Information Management*. ARMA International, May-June 2014. p.42-44. Web. 17 Dec. 2014.

[10] For more information, see *Recommendations for Implementation of Cloud Computing Solutions*. Federal Bureau of Investigation, Criminal Justice Information Services Division, Clarksburg,WV: 2012. Web. 17 Dec. 2014. and "Criminal Justice Information Services Security Policy." FBI.gov. Ed. CJIS Information Security Officer. *Criminal Justice Information Services*, 4 Aug. 2014. Web. 17 Dec. 2014. Version 5.3. CJISD-ITS-DOC-08140-5.3

data and records requirements. Courts should enlist the assistance of outside expertise to ensure that the terms and conditions of a cloud services agreement meets their needs and provide protection in the event of a vendor's failure to perform.

Implementation Considerations

The following are guidelines to consider before adopting a cloud-based solution:

Stakeholders

Include primary record stakeholders (clerk, technical staff, court administration, external users) in the planning, acquisition, deployment, and use of cloud computing solutions. These individuals should be fully informed about the impact of transition to the new environment, including anticipated changes in work processes and personnel.

Requirements

Clearly define the requirements for all record types, including interoperability with other systems, indexing, metadata, access, preservation, and destruction. Vendor obligations for system availability and allowable down time for maintenance should be clearly stated. Ensure that the provider and system are capable of meeting these requirements.

Licensing and Service Costs

Carefully review licensing and service costs, including start-up costs, termination fees, additional service/storage charges, etc. Some services will offer lower initial fees which go up after a period of time. Fees based on storage level thresholds should be clear, as costs per unit of storage may increase (or decrease) with growth in volume.

Transition Costs

Keep in mind transition costs of moving to a cloud environment. Existing data may need to be organized, purged, or transitioned to open formats prior to transfer. The initial move towards cloud computing may place additional responsibilities on technical staff during the transition period. It may necessary to run parallel systems for a period of time to ensure that the cloud-based system is working as intended.

Documentation

Develop documentation on how all records will be captured, managed, retained, and made available to authorized users, and the retention periods applied so that both the vendor and users have a clear understanding. This information will prevent future confusion over the responsibilities of each party and system performance requirements.

Auditing for Compliance

Establish a system for periodic audits of records and data to ensure compliance with stated requirements and standards for access, preservation and security. The adoption of existing industry standards should be considered in establishing performance benchmarks.[11]

Data Migration

For records with long-term retention periods (over 10 years), determine how data will be migrated to new formats, operating systems, etc., to maintain the accessibility and integrity of these records throughout their required life cycles. If records are required or allowed to be transferred to another agency, such as a state archives, include provisions for transfer of these records from the cloud.

Portability and Accessibility

Address potential issues with portability and accessibility through good records management policies and other data governance practices, and ensure that governance policies apply to information resources maintained in the cloud environment.

The importance of good information governance cannot be overstated in today's technical environment. The increasing complexity of information management requires managers to have a clear view of how their environment should operate and what is expected from the organization's systems and applications. This is true whether these systems are run internally or served by cloud providers.

Conclusion

The decision to utilize cloud services is often based on a presumption of reduced technical staffing and costs for IT services. While this may be the case in many situations, the move will likely require the organization to develop new technical skills and to increase emphasis on vendor management. This will include monitoring the

[11] The International Organization for Standardization (ISO) has recently issued cloud computing standards, ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary and 17789:2014 Information technology -- Cloud computing -- Reference architecture. U.S. National Information Standards and Technology agency (NIST), under the U.S. Department of Commerce, has published a number of standards and guidance documents on cloud computing, including NIST Cloud Computing Standards Roadmap.

vendor’s compliance with contractual obligations to ensure the court is receiving the services for which it is paying.[12] Regardless of the level of adoption of cloud services, good IT governance is an essential element of success.

Greater reliance on cloud computing as a means of delivering information services may be a substantial paradigm shift for some courts from the usual way of doing business. This shift must begin with a clear strategy, well-defined objectives, and measurable outcomes. However, planning for new technology and new approaches to information management is more than a technical exercise. It will require a change management strategy that takes into account not only the technical changes but the impact on business processes and the organization’s most important asset, its people.

[12] " Cloud Control – Managing Data in the Cloud Requires the Right Touch." *PC Today* 9.10 (2011): 20-22. Oct. 2011. *Internet Archive.* Web. 7 Nov. 2014.