Digital Records Pathways:
Topics in Digital Preservation

Module 8: Cloud Computing Primer

InterPARES / ICA
DRAFT July 2012

Table of Contents

Table of Figures

Digital Records Pathways: Topics in Digital Preservation

1 Preface

Digital Records Pathways: Topics in Digital Preservation is an educational initiative developed jointly by the International Council on Archives (ICA) and the International Research on Permanent Authentic Records in Electronic Systems Project (InterPARES). It offers training to archivists and records professionals in the creation, management and preservation of authentic, reliable and usable digital records. The program assumes that the user has a solid grounding in basic concepts of records management and archival theory, and builds on that knowledge.

Consisting of eight independent modules, *Digital Records Pathways* addresses the theoretical and practical knowledge needed to establish the framework, governance structure and systems required to manage and preserve digital records throughout the records' lifecycle.. Each module addresses a specific topic of relevance to the management and preservation of digital records. The program is provided free of charge on the ICA website at www.ica.org/.

1.1 About the ICA and InterPARES

The ICA and InterPARES are committed to establishing educational materials for the continuing education of archivists and records managers, to build upon foundational knowledge, disseminate new findings, and to equip archivists and records professionals with the necessary specialized knowledge and competencies to manage and preserve digital records.

The International Council on Archives (ICA) (www.ica.org) is dedicated to the effective management of records and the preservation, care and use of the world's archival heritage through its representation of records and archives professionals across the globe. Archives are an immense resource. They are the documentary by-product of human activity and as such an irreplaceable witness to past events, underpinning democracy, the identity of individuals and communities, and human rights. But they are also fragile and vulnerable. The ICA strives to protect and ensure access to archives through advocacy, setting standards, professional development, and enabling dialogue between archivists, policy makers, creators and users of archives.

The ICA is a neutral, non-governmental organization, funded by its membership, which operates through the activities of that diverse membership. For over sixty years ICA has united archival institutions and practitioners across the globe to advocate for good archival management and the physical protection of recorded heritage, to produce reputable standards and best practices, and to encourage dialogue, exchange, and transmission of this knowledge and expertise across national borders. With approximately 1500 members in 195 countries and territories the Council's ethos is to harness the cultural diversity of its membership to deliver effective solutions and a flexible, imaginative profession.

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) (www.interpares.org) aims to develop the knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form and provide the basis for standards, policies, strategies and plans of action capable of ensuring the longevity of such material and the ability of its users to trust its authenticity. The InterPARES project has developed in three phases:

InterPARES 1 (1999-2001) focused on the development of theory and methods ensuring the preservation of the authenticity of records created and/or maintained in databases and document management systems in the course of administrative activities. Its findings present the perspective of the records preserver.

InterPARES 2 (2002-2007) continued to research issues of authenticity, and examined the issues of reliability and accuracy during the entire lifecycle of records, from creation to permanent preservation. It focused on records produced in dynamic and interactive digital environments in the course of artistic, scientific and governmental activities.

InterPARES 3 (2007-2012) built upon the findings of InterPARES 1 and 2, as well as other digital preservation projects worldwide. It put theory into practice, working with archives and archival / records units within organisations of limited financial and / or human resources to implement sound records management and preservation programs.

1.2 Audience

The audience for this program includes archivists and records and information professionals interested in expanding their competencies in the management of digital records. Taken as a whole, the modules form a suite of resource materials for continuing professional education with particular focus on issues influencing the preservation of reliable, accurate and authentic digital records.

1.3 How to Use the Modules

Each module consists of theoretical and methodological knowledge and its practical application, illustrated through case studies and model scenarios. While the modules have been developed by InterPARES Team Canada, and are therefore illustrated with examples from the Canadian context, each module is customizable for a specific domain or juridical context. For wider applicability, they have been translated into the languages of the ICA partners.

The modules can be studied individually according to need and interest, or as a set, covering the range of competencies required. They can be self-administered by individuals, or offered through professional associations or workplace training. The modules also contain a number of templates that allow universities and professional associations to adapt and to develop specific course curricula, on-site training materials for students and professionals on digital recordkeeping and preservation issues. Universities and professional associations are free to adapt the materials and develop their own context-specific course curricula and training kits.

1.4 Objectives

The modules have the following objectives:

- To provide educational resources based on cutting edge research in digital records issues to professional archival and records management associations for the benefit of their members;
- To provide archivists and records managers with the necessary theoretical knowledge as well as procedural and strategic skills to develop, implement and monitor a digital recordkeeping and/or a preservation program;
- To illuminate theoretical concepts with practical applications through real life examples drawn from case studies, anchored in specific administrative and technological contexts;
- To provide university programs with content and structure for courses on digital records management and preservation.

1.5 Scope

Digital Records Pathways: Topics in Digital Preservation consists of the following modules:

Module 1: Introduction – A Framework for Digital Preservation
Module 2: Developing Policy and Procedures for Digital Preservation
Module 3: Organizational Culture and its Effects on Records Management Selection and Appraisal of Digital Records
Module 4: An Overview of Metadata
Module 5: From *Ad Hoc* to Governed – Appraisal Strategies for Gaining Control of Digital Records in Network Drives
Module 6: E-mail Management and Preservation
Module 7: Management and Preservation of Records in Web Environments
Module 8: Cloud Computing Primer

Each module consists of some or all of the following components as appropriate:

- **Overview** of the topic and scope of the module;
- **Learning objectives** and expected level of knowledge upon completion;
- **Methodology** or the procedures to follow in order to apply the module;
- **Templates (where appropriate)** to facilitate the implementation of the module;
- **Case Study(ies)/Scenarios (where appropriate)** that provide real-world examples of module topic
- **Exercises** covering key learning points;
- **Review questions** to enhance comprehension and understanding of the topic;
- Additional **Resources** for the topic, including **readings, standards** and other **templates** for reference

Overview of the set			
1. A Framework for Digital Preservation 2. Developing Policy and Procedures for Digital Preservation			Foundational
3. Organizational Culture	4. An Overview of Metadata	5. Appraisal Strategies	General purpose
6. E-mail	7. Websites	8. Cloud Computing	Specific purpose
International Terminology Database			Foundational

1.6 International Terminology Database

The terminology used in the modules reflects common usage in archival and records management communities of practice. To ensure common understanding, and minimize potential confusion that may arise from regional or jurisdictional practice, all modules are supported by the International Terminology Database, available at http://www.web-denizen.com/. As well, certain specific terms are included in short glossaries in each module.

Module 8 – Cloud Computing Primer

2 Introduction

Cloud computing consists of on-demand computing services delivered over the Internet from a remote location or via an organisation's servers. Still an emerging concept, it is reflective of the shift from the client-server model to the network model; from isolated environments to the Internet; it enables a platform and location-independent perspective for communication, collaboration, storage and production.

The basic idea behind the cloud is that anything that can be done on in-house computing systems, from storage and collaboration to processing and communication can be shifted to the cloud – at its core, cloud computing is a service or set of services delivered over the Internet, on demand, from a remote location rather than residing on a desktop/laptop or organisation's servers. Organisations contract with a service provider to deliver storage, processing and/or applications via the web. Cloud computing resources are location- and device-independent – affording for ready, on-demand access to information, applications and processing from any location.

Cloud computer offers flexibility and convenience – as long as there is access to the web, users are able to work when and where they want, it doesn't matter where the data on the screen comes from. Additionally, cloud computing enables providers to use distant data centers for cloud computing.

Cloud computing is rapidly being adopted by public and private organisations due to its potential perceived benefits, including cost efficiency, scalability, convenience and performance. However, the potential risks of adopting cloud computing must be fully understood before it is adopted by organisations in order to make informed decisions around its utilization.

2.1 Aims and Objectives

- The purpose of this module is to define the characteristics of cloud computing and explain its service and deployment models, outline a methodology and identify tools for analyzing the risks when employing the cloud within your organisation;
- This module lays the groundwork to aid users in developing a cloud computing strategy and identifying records and processes that are potential candidates for outsourcing to the cloud;
- This module aids users in identifying the issues relevant to the use of cloud computing when selecting processes, applications and records to be moved to the cloud and business requirements, rules and compliance frameworks that must be examined in light of the issues cloud computing raises

2.2 Scope

This module provides a primer on cloud computing and the associated records management issues and challenges that should be considered before an organisation

moves its records and/or services to the cloud. It is not intended to act as a risk analysis or policy development tool, but to aid users in developing an organisational cloud computing strategy.

2.3 Learning Outcomes

Upon completion of this module, you will be able to:

- Identify and understand the essential characteristics cloud computing;
- Identify and understand the three cloud computing service models;
- Identify and understand the four deployment models of cloud computing;
- Understand the potential benefits of cloud computing;
- Understand the potential risks and issues involved in utilizing cloud computing;
- Understand strategies for identifying the risks in employing cloud computing utilities within your organisation and ask key questions to aid in determining such risks;
- Know where to locate additional information and resources that will facilitate understanding and implementation of cloud computing technologies.

3 Overview

3.1 Definition of Cloud Computing

The National Institute of Standards and Technology (NIST) currently provides the most comprehensive and widely adopted cloud computing definition. This definition identifies five essential characteristics of cloud computing, three services models and four deployment models. Following is the NIST cloud computing definition:

> Cloud computing is 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 services provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

3.1.1 Essential Characteristics

On-demand self-service: users can provision computing capabilities (e.g. server time and network, storage, etc.) as required without assistance from service provider

Broad network access: availability over the network with access via standard internet-accessible devices (e.g. mobile phones, laptops, etc.)

Resource pooling: a multi-tenant model that pools resources between users

Rapid elasticity: ability for users to rapidly increase or decrease cloud capabilities on-demand

Measured service: resource use is monitored, controlled and reported, allowing users are charged based on their usage for each type of service (e.g. storage, processing, bandwidth, etc.)

3.1.2 Service Models

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based email). The consumer does not manage or control the underlying cloud infrastructure including 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 and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including networks, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

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).

3.1.3 Deployment Models

Private cloud: The cloud infrastructure is operated solely for an organisation. It may be managed by the organisation or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organisations and supports specific community that has shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be managed by the organisations or a third party and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organisation selling cloud services.

Hybrid cloud: The 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 that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

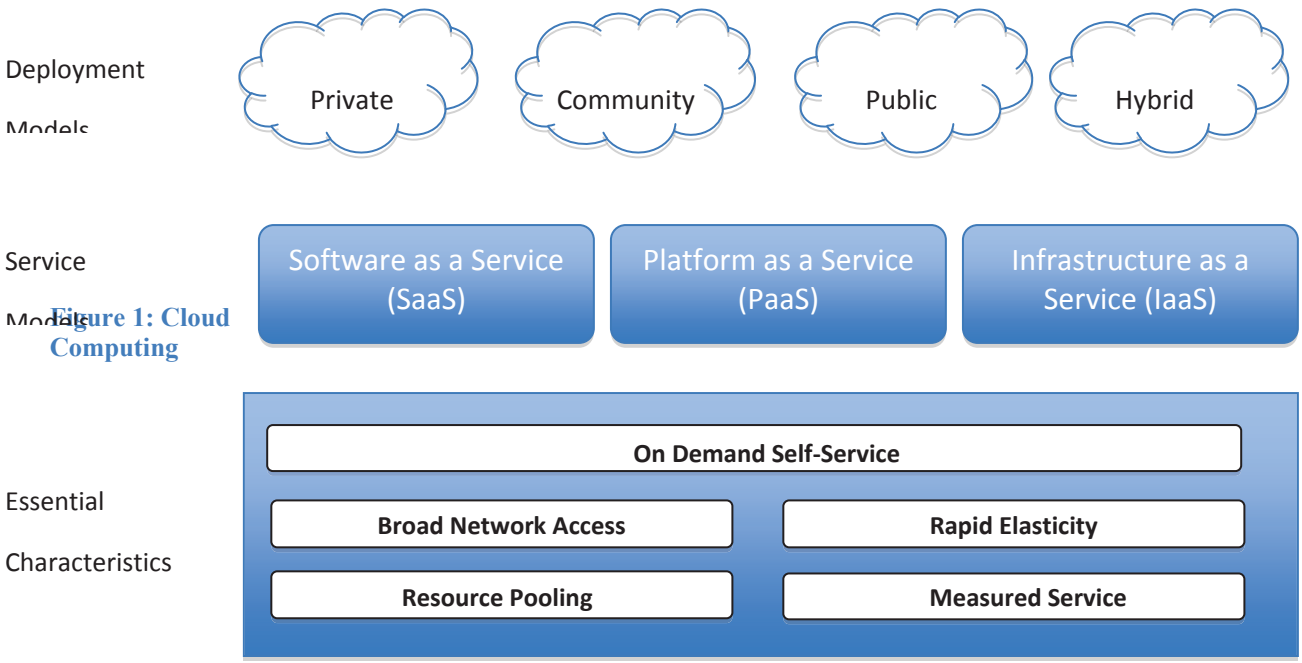

Figure 1: Cloud Computing

Adapted from NIST. (2009) *Presentation on Effectively and Securely Using the Cloud Computing Paradigm v26.* Available at http://csrc.nist.gov/groups/SNS/cloud-computing/ and Nicole Convery. *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*. Available at www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

4 Key Issues in the Adoption of Cloud Computing

The potential benefits for an organisation in moving information and business processes into the cloud are numerous, however, much depends on the organisational context in which the cloud services are deployed and the choice of cloud computing services and models chosen. Moving information and services to the cloud is not without its risks and challenges. While issues of security and availability are common concerns with cloud computing in general, a number of other challenges will depend on the cloud environment and services chosen by the user. Those contemplating moving information and services to the cloud need to gain a full understanding of the benefits and risks associated with cloud computing and mitigate risks by adopting a risk-based approach in planning which of their records and/or processes are best suited to the cloud environment.

4.1 Scalability

Employing cloud computing allows organisations to leverage shared infrastructure and take advantage of economies of scale. "Cloud computing turns the economics of IT on its head, due to an unprecedented elasticity of resources" (Wyld, 2009). Users can provision cloud computing resources on-demand, eliminating the requirement for predetermined usage forecasts, scaling up services when organisational demand is at its peak and scaling back during less demanding cycles. Scalability is "the ability of a computing system to grow relatively easily in response to increased demand" (Langley, 2008). Such a shift to IT as a utility model can provide benefits to organisations through aggregated sharing of resources across platforms and can eliminate large investments in in-house infrastructure and software. Cloud computing solutions are ideal in situations that experience spikes in demand for computing resources – in both the public and private sectors – where shifts in demand for resources can range from little or no demand to the need to handle large amounts of data or processing. Scalability benefits can be ensured as long as cloud computing usage is monitored and, if necessary, regulated by organisations to ensure cost benefits are realized (Convery, 2010).

4.2 Resiliency and Reliability of Service

Cloud computing providers can often offer enhanced reliability relative to more traditional in-house IT services. Because cloud computing providers possess large computing resources, server failure rarely impacts the services provided to users as applications and services can be automatically rerouted to different servers. User information is often redundantly stored on various servers in multiple locations aiding in the prevention of loss of information in the event of a data centre disruption or outage. This idea of no single point of failure, provides users with a high degree of resiliency in computing resources. Cloud service providers often guarantee a certain benchmark of availability of services in what are known as Service Level Agreements (SLAs), often for up to 99.99% of the time (translating into just 52 minutes downtime per year). Addition of nines often sees the costs in the SLA rise.

Despite the high level of guarantee of service by cloud providers, most organisations are reluctant to use the cloud for the storage of "mission-critical" data and information, regardless of the financial and efficiency benefits. Cloud computing providers do have outages (e.g. Gmail had an outage of 100 minutes in September 2009), which are beyond the control of the user. Additionally, cloud providers are more prone to hackers or malicious insiders and must be able to react to such threats quickly and effectively. While SLAs will provide for compensation in the event of an outage, liability for any damage resulting from the outage will rest with the user and if such an outage occurs at a critical juncture, compensation could mean little in light of the reputational and future business losses incurred due to such an outage (Convery, 2010). Allocation of resources by the cloud provider can also impact the reliability of service for users. An underestimation on the part of the provider can result in a slow down or interruption in service to users.

Cloud computing is still in its relative infancy, and as such, there are no general standards or regulated guidelines for interaction with users. As a for-profit business model, cloud providers are subject to market conditions, acquisitions, takeovers, etc. If a cloud

computing provider suddenly goes out of business or is bought up by another company, changes to services can occur unexpectedly and have a negative effect on organisations who utilize their services and applications – including loss of information, interruption in business operations and/or customer services, etc. Organisations should investigate a cloud provider's reputation, history and potential sustainability before deciding to sign on.

4.3 Efficiency and Ease of Use

The nature of cloud computing affords for easy and near immediate access to services and applications as compared to the more traditional organisational model of hardware/software purchase, installations and deployment. Because services and applications are located "in the cloud" users can access them from virtually anywhere they can access the Internet. Additionally, cloud computing allows organisations to "test drive" services and applications without large expenditures and with minimal financial loss if terminated. The cloud environment can afford for new technological and/or economic solutions for users which were not feasible without cloud computing and the efficiency provided by the cloud can allow for the reallocation of IT services to other tasks.

4.4 Cost

Because infrastructure resources are shared across large numbers of applications and users, cloud computing can greatly diminish or eliminate organisational infrastructure purchase and maintenance costs. Cloud computing use can result in reduced spending on information and communication technologies as organisations are not required to make large capital expenditures but can employ an on-demand purchase model, only purchasing those computing resources they require to conduct business at any given time. Organisations can treat cloud computing applications and services as operational rather than capital expenses. Organisational use of cloud computing resources reduces operating costs through the reduction or reassignment of in-house IT personnel, more effectively utilizing human resources. Further cost efficiencies come from the reduction in energy consumption, the reduction in time wasted due to delays in computing operations, and the reduction in wasted resources such as unused server space. Despite these apparent cost savings, organizations must calculate the total costs involved that will be incurred by moving records and services to the cloud (including an examination and assessment of the cloud providers' pricing structure), undertaking a cost benefit ratio analysis to identify the real costs before moving records and services to the cloud.

4.5 Interoperability and Integration

Cloud computing is an emerging industry. There is a current lack of standardization,[1] and the use of proprietary interfaces and software in the cloud industry is in the cloud provider's best interests as it works to keep customers locked in (Convery, 2010). This

[1] There are initiatives such as www.cloud-standards.org working to standardize APIs and procedures.

lack of standardized interfaces and procedures may hinder an organisation's ability to effectively combine a variety of cloud services between multiple providers and move information between cloud providers. Organisations need to employ strategies of open standards, interoperability and information portability in order to avoid and/or mitigate vendor lock in. Despite the outsourcing of applications and services, depending on the cloud model chosen, the level of management and maintenance on the part of the organisation can fluctuate.

The integration of cloud services into an organisation's existing IT environment should also be taken into consideration as it will require IT resources. Moving to the cloud impacts on existing architecture, particularly where new cloud applications and services will interface with existing organisational systems. Cloud computing services may limit the opportunities for customization of applications and services, increasing the complexity of integrating these into existing systems. An evaluation of the impact on existing business processes is necessary prior to moving to the cloud to ensure any technical barriers are addressed.

4.6 Compliance and E-Discovery

The storage of information in the cloud must take into consideration compliance with data protection legislation applicable to the juridical context of the organisation involved. Issues of where information is stored, the security measures in place to protect the information, the ability to access the information and the ability to ensure its authenticity are all issues that must be taken into consideration by cloud users.

Information stored across jurisdictions may be vulnerable to disclosure and seizure by foreign governments or agencies whose legislation may be in conflict with that of the originating organisation. Because cloud services operate on the principle of shared multi-tenant environments, information stored in the cloud may be in jeopardy of disclosure or seizure due to its proximity to other users' information that is sought in legal action. "The USA Patriot Act, the Homeland Security Act, and other related security legislation, coupled with sophisticated electronic information-gathering technologies, make it possible for governments to gain access to electronic information in virtually any context" (Jaeger, Lin & Grimes, 2008). A variety of legal issues can arise regarding information stored on remote servers including the gathering of data that is "several degrees" removed from the intended subject (Jaeger, Lin & Grimes, 2008) as well as innocent but sensitive organisational information getting caught up in an investigation (Jaeger, Lin & Grimes, 2008). Cloud users need to be aware of their jurisdictional legislative and regulatory requirements and ensure information stored in the cloud is in compliance with these..

In cases of litigation, users of cloud applications and services must be able to effectively locate and retrieve information from the cloud in the discovery process without damage to the authenticity and integrity of this information. Due to the dynamic nature of the cloud, locating information at any given point in time may be difficult and impact on timely retrieval of information.

The relative newness of cloud computing services means that most existing security and compliance standards are not designed to address the cloud environment and can affect certification and liability on the part of the cloud user.

Exercises:

- Identify the legislative and regulatory frameworks that apply to the records in your organisation.
- How would storing records in the cloud potentially impact on your organisation's ability to comply with these laws and regulations?

4.7 Business Continuity and Disaster Recovery

Cloud computing can provide inexpensive and effective business continuity and disaster recovery strategies for organisations. Organisations can utilize the cloud infrastructure to facilitate redundancy of information stored offsite, greatly reducing hardware costs associated with traditional back up and disaster recovery models.

Internet service interruptions may affect cloud services and disrupt business continuity. The dynamic nature of the cloud may mean that information stored in there is not immediately available in the event of a disaster. Additional costs may be incurred due to monitoring and security services required in order to meet compliance obligations. Business continuity and disaster recovery planning must be planned, tested and documented.

4.8 Privacy and Confidentiality

Unauthorized access to private and confidential data is a privacy concern for information residing in the cloud. User data may reside in multiple jurisdictions that may pose risks to the security of personal and confidential data. Data centres residing in "high-risk" locations may be subject to "unpredictable legal and enforcement frameworks" and can mean personal data is susceptible to third-party, unauthorized access. The responsibility for keeping information secure is transferred to the cloud provider in a cloud computing environment, yet liability for safeguarding personal and confidential information resides with the cloud user as the collector of the information.

It may be difficult for cloud users to effectively check the data handling and processing techniques of the cloud providers to ensure that data is handled lawfully and in accordance with the user's requirements. As the "controller" of the information, the cloud user is responsible for the security of the personal and confidential information it collects, even if mishandling of personal and confidential data is on the part of the cloud provider. Ensuring service providers meet the requirements of privacy legislation and employing a "robust access and authentication management regime" and good encryption of data

(Convery, 2010) can aid in ensuring the protection of personal and confidential information residing in the cloud.

4.9 Intellectual Property and Copyright

Because the Internet crosses international domains, the application of intellectual property and copyright law can be a broader and more difficult to navigate issue when information is stored in the cloud on remote servers. Difficult questions arise about which laws apply to this information and the responsibilities of the organisation that creates and owns this information.

Unauthorized disclosure of trade secrets can be an issue for organisations storing information in the cloud.

4.10 Integrity of Information

Most cloud architectures lack formal standards governing how data is stored and manipulated and many cloud applications lack the record functions common on in-house applications, making it difficult for users to meet records management requirements.

Authenticity and reliability of information are linked to the ability to demonstrate its chain of custody. Much of the responsibility for information storage and processing in the cloud environment resides with the cloud provider. Maintaining authenticity (or the appearance of authenticity) may be difficult to maintain in a cloud environment as it is more susceptible to unauthorized access as a result of interception via transfer over unsecure networks, comingling with other data in multi-tenant environments, and ineffectual destruction.

4.11 Loss of Governance

Cloud computing use increases the need for governance. “Governance implies control and oversight over policies, procedures, and standards for application development, as well as design, implementation, testing and monitoring of deployed services” (Jansen & Grance, 2011). Due to the nature of cloud computing, and the ability of users (employees) to easily engage in could computing services, lack of organisational control is a real possibility in the cloud environment. Responsibilities for information security for information stored in the cloud are transferred to the cloud provider. The amount of control a cloud user has over security often depends on the cloud service model chosen – ranging from little or no control over SaaS provider infrastructure to more control of applications and systems in an IaaS environment.

Loss of governance can result in an inability on the part of organisations to comply with legislative and regulatory requirements and an inability to demonstrate the authenticity and reliability of information that is stored in the cloud (Convery, 2010).

4.12 Data Ownership

Establishing organisational ownership of information stored in the cloud is an essential component of the service agreement. As data residing in social media sites has illustrated,

data ownership and privacy rights can fall victim to ambiguous service agreements. Organisations should ensure they maintain ownership rights and that the cloud provider does not acquire ownership, licensing or use rights over the organisation's information.

4.13 Information Retrieval and Destruction

Records management practices require that routine destruction of records occur in order to comply with an organisation's retention schedule. Achieving effective records destruction may be difficult to achieve in the cloud environment. Insecure or incomplete data deletion is an issue in the cloud environment and "adequate and timely data deletion may be impossible" due to the unavailability of extra stored copies or because the multi-tenant model of the cloud may have client data sharing disk space (ENISA, 2009). Organisations can enlist encryption keys and other methods to aid in achieving compliant and effective destruction of records stored in the cloud.

While replication of information in various locations in the cloud for means of redundancy can benefit organisations, compliance with Freedom in Information and Access and Protection of Privacy legislation requires organisations to be aware of how many copies of their information exists and where it resides in order to comply with such legislation.

"If information extraction requires a change of format of information, this can have serious consequences for the authenticity and reliability of corporate records and impact on their legal admissibility" (Convery, 2010).

See Appendix A for ten questions to ask when outsourcing to the cloud.

5 Cloud Computing Readiness – Assessment and Preparation

Cloud computing is a tool which will need to fit into the overall IT strategy of an organisation and aid in supporting the mission and overall business strategy of the organisation. Outsourcing records storage and organisational processes to the cloud environment can benefit organisations through cost savings, scalability and convenience. An organisational assessment of which records, processes and applications can be effectively migrated to the cloud environment must take into consideration an organisation's business requirements, risk and compliance frameworks (Convery, 2010).

See the "Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud" at www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Utilizing a decision framework to assess your organisation's cloud computing readiness in preparing to migrate records and services to the cloud will help to identify any issues and aid in identifying which records and processes are best suited for the cloud environment.

5.1 Cloud Computing Decision-making Framework

The cloud computing decision-making framework is divided into the following phases:

1. Gathering data about cloud computing service and deployment models, and cloud computing providers;
2. Conduct an organizational assessment to identify which records, applications and process candidates for migration to the cloud environment;
3. Determine which cloud service and deployment models fit your organization's business drivers and governance and compliance requirements;
4. Conduct a risk assessment of the records, applications and processes moving to the cloud, including identifying, analyzing and developing a response plan for risk;
5. Conduct a cloud pilot or organization cloud rollout, moving identified records, applications and processes to the cloud environment;
6. A number of issues must be taken into consideration and planned for with the ongoing management of records, applications and processes moved to the cloud – including records management and classification; compliance, monitoring and auditing, security and ongoing access;
7. Before moving any records, applications or processes to the cloud, organisations must ensure procedures are in place to retrieve information from the cloud provider's systems and transfer them to another service provider or the organization.

The cloud computing decision-making framework is a series of steps, some of which are iterative and may occur concurrently. The following subsections expand on each phase of the framework.

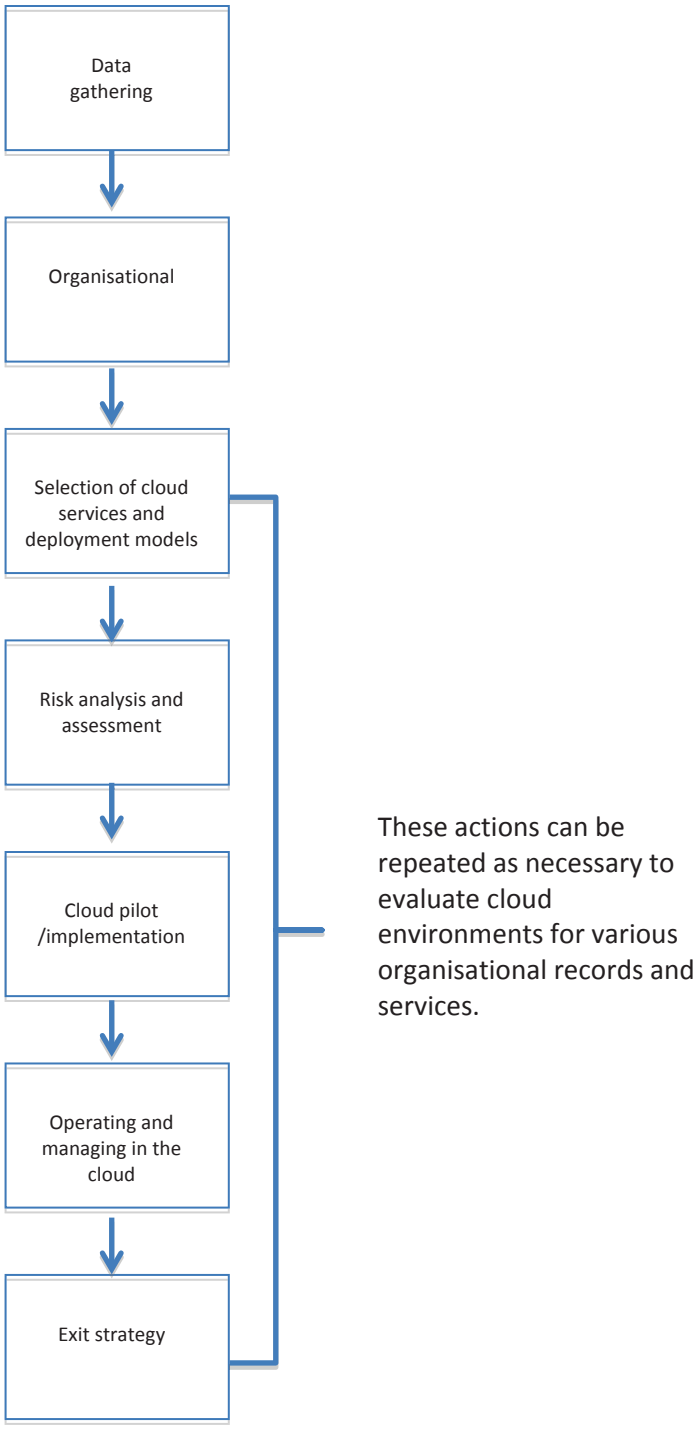

Figure 2: Cloud computing decision-making framework

5.2 Data Gathering

The decision-making framework begins with learning the fundamentals of cloud computing. Reading available definitions and resources, attending seminars and/or workshops and speaking with cloud computing vendors will assist individuals in gaining a thorough understanding of cloud computing and its various models. It is important to ensure that it is not just the IT personnel that are educated on how cloud computing works, but also that policy and decision makers are informed.

A number of available resources are listed in section six which will aid users in gaining an understanding of cloud computing and the issues involved in its adoption. Many of the resources listed in this section include bibliographies leading to a broader network of resources.

Exercise:

- Identify the policy and decision makers in your organisation who would be candidates for cloud computing education.

5.3 Organizational Assessment

In order to successfully take advantage of the benefits of migrating records, applications and processes to the cloud, organisations must identify which of their organisation's records and processes are suitable for the move.

The level at which organisations performs evaluations of which assets to move to the cloud will vary in detail depending on their business requirements and regulatory and compliance frameworks. Organisations may have an existing framework they utilize to assess potential outsourcing projects that may be suitable to the task. Alternately, internal data gathering will aid organisations in assessing assets appropriate for the cloud environment.

Convery (2010) identifies a number of organisational applications and processes that are often suited to migration to the cloud environment due to cost savings and better efficiency or functionality. These include:

- Email;
- Document management;
- Collaboration tools;
- Productivity tools (e.g. payroll systems);
- Long-term storage of inactive information.

Conducting a contextual analysis will aid in identifying records, applications and processes that can be safely moved to the cloud. Such an analysis can take place at an organisational level or could be conducted in the context a business function or organisational unit. A contextual analysis gathers information about the organisation, its administrative structure; its legal and regulatory obligations with respect to its records; norms and standards which influence record creation; maintenance and use; its record creating and recordkeeping requirements and constraints, including the business culture of the organisation, personnel constraints and technological constraints.

See Appendix B: Contextual Analysis

Gain a comprehensive understanding of the current practices of records creation and management in your organisation by interviewing records creators and analyzing relevant policies that govern and constrain records management. Examine all standards and best practices relevant to your organisational context.

See Appendix C: Records Analysis

Using your organisation's classification framework can aid in identifying records and/or information to be transferred, processed and stored in the cloud. Once information has been have been identified it should be assessed in terms of breaches to confidentiality, integrity and availability to help identify acceptable organisational risk parameters for information stored in the cloud (Convery, 2010).

Security Objectives	Potential Impact		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.

(Convery, 2010, adapted from: Categorization of federal information and information systems from NIST (2008) Information security. Vol. 1: Guide for mapping types of information and information system categories. NIST SP800-60. Online. Available at: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800_Vol1-Rev1.pdf)

Exercises:

- Are there records in your organisation that could be effectively moved to the cloud? Identify them.
- Which records in your organisation would you advise against moving to the cloud? Why?
- What applications and/or services currently undertaken in-house in your organisation could be moved to the cloud? Why are these best suited to the cloud?

5.4 Selection of Cloud Computing Service and Deployment Models

Once you have identified the records, applications and processes that can be migrated to the cloud, determine which cloud service and deployment models fit your organisation's business drivers and governance and compliance requirements (Convery, 2010).

Employing a SWOT analysis – identifying the strengths, weaknesses, opportunities and threats for each cloud model – can be an effective approach in determining which combination of cloud deployment and service models will best suit your organisation's needs (ENISA, 2011).

There are significant trade-offs to each service model in relation to integrated features, complexity vs. openness (extensibility) and security.

- SaaS provides the most integrated functionality with the least extensibility and a relatively high level of integrated security;
- PaaS tends to be more extensible than SaaS at the expense of "customer-ready" features and capabilities, but there is more flexibility to layer on additional security;
- IaaS provides few if any application-like features, but large extensibility. Meaning less integrated security beyond protecting the infrastructure. Operating systems, applications and content are managed and secured by the consumer.

Organisational reasons for migrating records, applications and/or processes to the cloud should inform the organisation's cloud computing strategy, taking into account the organisation's business and IT strategies (Convery, 2010). The selection of cloud service and deployment models must also take into consideration the degree of control an organisation will have over security and risk.

5.5 Risk Analysis and Assessment

Conduct a risk assessment of the records, applications and processes moving to the cloud, including identifying, analyzing and developing a response plan for risk.

It is important to understand the organisational value of the information, records and/or system that you are seeking to move into the cloud. Carrying out a context specific risk analysis will aid organisations in assessing the risk of moving records and process to the cloud and aid in preparing for effective adoption of cloud computing.

ENISA's "Information Assurance Framework" is an excellent resource for assessing risk in the adoption of cloud computing, comparing cloud providers, and preparing for effective adoption. The Framework provides a set of questions that an organisation can ask a cloud provider to effectively ensure they are protecting the information entrusted to them (these are meant to serve as a baseline and should be

augmented by an organisation's individual requirements). Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

5.6 Cloud Pilot/Implementation

Conduct a cloud pilot or organisation cloud rollout, moving identified records, applications and processes to the cloud environment. Closely monitoring of a pilot will ensure that unforeseen issues are identified and addressed early in the process. The initial pilot process may be iterative until confidence is established that the chosen platform and/or service meet all necessary requirements.

5.7 Operating in the Cloud

A number of issues must be taken into consideration and planned for with the ongoing management of records, applications and processes moved to the cloud – including records management and classification; compliance, monitoring and auditing, security and ongoing access.

5.8 Exit Strategy

Before moving any records, applications or processes to the cloud, organisations must ensure procedures are in place to retrieve information from the cloud provider's systems and transfer them to another service provider or the organisation.

6 Review Questions

1. Name the five characteristics of cloud computing.
2. Identify and explain the three cloud service models.
3. Identify and explain the four cloud deployment models.
4. What are the benefits and risks of utilizing the cloud impact to enhance business continuity and disaster recovery?
5. How can utilizing the cloud environment be cost effective for organisations?
6. List five benefits for organisations in moving applications and services to the cloud.
7. List five risks for organisations in moving applications and services to the cloud.

7 Additional Resources

Author: Australian Government, Department of Finance and Deregulation
Title: Cloud Computing Strategic Direction Paper
Publication Date: January 2011
URL: http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

This paper describes the Australian government's position on cloud computing. The Australian government strategy allows agencies to choose cloud-based services if they demonstrate financial value, are fit for the purpose and are adequately secure. The paper also provides guidance on what cloud computing is, identifies issues and benefits of cloud computing for agencies. The government's strategy is divided into three streams – agency guidance and documentation; cloud adoption for "unclassified" services and study the risks; and encourage strategic approaches to cloud computing.

Author: Convery, Nicole
Title: Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud
Publication Date: August 26, 2010
URL: www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

An excellent resource, this investigative and comprehensive toolkit is a must- read for information and records professionals investigating the option of cloud computing for their organizations.

Author: Wyld, David c.
Title: Moving to the Cloud: An Introduction to Cloud Computing in Government
Publication Date: 2009
Source/Publisher: IBM Center for The Business of Government: E-Government Series
URL: http://www.businessofgovernment.org/report/moving-cloud-introduction-cloud-computing-government

An examination of the state of cloud computing in U.S. government organizations and the potential benefits and drawbacks of the government use of cloud computing. Provides a general introduction to cloud computing terminology, models and frameworks.

Author: ENISA
Title: Security & Resilience in Government Clouds: Making an Informed Decision
Publication Date: January, 2011
Source/Publisher: ENISA
URL: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds

Author: Cloud Security Alliance
Title: Security Guidance for Critical Areas of Focus in Cloud Computing
Publication Date: December 2009
Source/Publisher: Cloud Security Alliance
URL: https://cloudsecurityalliance.org/guidance/

This report investigates the security issues relevant to the cloud, providing analysis and guidance on decisions around security in the cloud.

8 References

Askhoj, J., Sugimoto, S., & Nagamori, M. Preserving Records in the Cloud. Preprint.

Armbrust, M., et al.. (2009). Above the Clouds: A Berkeley View of Cloud Computing.

Australian Government Department of Finance and Deregulation. (April, 2011). Cloud Computing Strategic Direction Paper. Available at http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

Australian Government, Department of Innovation, Industry, Science and Research. (October, 2011). IT Industry Innovation Council. Cloud Computing – Opportunities and Challenges

Ball, C. (February, 2011). Facebook Feature Could Ease Cloud-Based EDD LTNLaw Technology News.

Bradshaw, S., Millard, C. & Walden, I.. (2010). Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, *Queen Mary School of Law Legal Studies Research Paper no. 63*.

BSA. (2011). Cloud Computing Policy Agenda for Europe.

Cloud Computing Explained by Rosalyn Metz. Educause Quarterly. Available at http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/CloudComputingExplained/206526

Cloud Security Alliance (CSA). (March, 2010) *Top Threats to Cloud Computing v.1.0.* Available at https://cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/

Convery, Nicole. (August 26, 2010). *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud* Available at www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Digital Agenda Assembly. (2011). Report from Workshop 18: Towards a Cloud ComputingStrategy for Europe: Matching Supply and Demand.

ENISA (November, 2009). Cloud Computing: Benefits, Risks and Recommendations for Information Security.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud Computing and Information Policy: Computing in a Policy Cloud?', *Journal of Information Technology & Politics*, 5(3), 269-283.

Maxwell, W. & Wolf, C. (May, 2012). A Global Reality: Governmental Access to Data in the Cloud: A comparative analysis of ten international jurisdictions Governmental access to data stored in the Cloud – including cross-border access – exists in every jurisdiction. *Hogan Lovells White Paper*.

NIST (2010) *Definition of Cloud Computing v15.* Online. Available at http://csrc.nist.gov/groups/SNS/cloud-computing/

O'Brien, K. J. (Sept. 19, 2010). New York Times. Cloud Computing Hits Snag in Europe.

Office of the Information and Privacy Commissioner of British Columbia. (February, 2012). Cloud Computing Guidelines for Public Bodies. Available at http://www.oipc.bc.ca/news/2012Releases/CloudComputing_Announcement.pdf

Pew Internet and American Life Project. (2010). The Future of Cloud Computing.

Stuart, K. & Bromage, D. (2010). Current state of play: records management and the cloud. *Records Management Journal.* 20(2), 217-225.

Wyld, D. C. (2010). The Cloudy Future of Government IT: Cloud Computing and the Public Sector around the world. *International Journal of Web & Semantic Technology*, 1(1).

Appendix A: Top 10 Questions when outsourcing to the cloud[2]

Nicole Convery provides a useful list of the top ten questions users should ask when contemplating outsourcing computing applications and services to the cloud.

- Which process, application and information can be moved to the cloud to gain efficiency and cost benefits while satisfying the organisation's security and compliance requirements?
- How can the organisation be harmed if systems, applications, services or information are accessed by unauthorised people and information is being made available to the public?
- How are information and systems protected against unauthorized access (e.g. hacking, interception, user misuse) by the cloud service provider?
- How can the organisation ensure the integrity, authenticity and reliability of information stored in the cloud?
- What are the organisation's responsibilities regarding the security of infrastructure and information in the cloud for the chosen cloud service and deployment models?
- How can the organisation apply its records and information management programmes (e.g. classification, retention) in the cloud environment?
- What is the impact of outsourcing services and information to the cloud on the legislative and regulatory requirements of the organisation (e.g. DP, FOI, SOX, e-discovery, copyright, licensing, etc.)?
- How should the organisation audit and monitor cloud services and establish relevant service level agreements?
- Will the organisation be able to negotiate contracts and agreements that fit their risk assessment and compliance environment?
- What are the total costs of setting up and managing the cloud services?

[2] Nicole Convery. "Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud." Department of Information Studies, Aberystwyth University. Archives & Records Association UK & Ireland. 26 August 2010.

Appendix B: Contextual Analysis

A contextual analysis gathers data about the organisation and its regulatory and legal frameworks. It includes information about the organisation's administrative structure; its legal and regulatory obligations with respect to its records; norms and standards which influence record creation, maintenance and use; its record creating and recordkeeping requirements and constraints, including the business culture of the organisation, personnel constraints and technological constraints. A contextual analysis provides the following information.

Legal and Regulatory Position

Identify and provide information about all laws and regulations, and legally required standards or codes of conduct that govern or affect your organisation's records creation and recordkeeping, including requirements for retention and disposition.

Norms

Identify and provide information about any non-legally required standards, methodologies, codes or regulations that govern or affect your organisation's records creation and recordkeeping, including requirements for retention and disposition.

Resources (Physical)

Summarize information about the physical context in which your organisation operates, including relevant information about equipment and infrastructure.

Governance

Document the governance structure of your organisation and the decision-making process as it relates to records management.

Provide the mission statement(s), which may have evolved over time.

Policies

Identify and provide information about all existing policies that pertain to records, their creation, maintenance, retention and disposition and long-term preservation.

Functions

List all of the major functions that your organisation undertakes that result in the creation of records.

Appendix C: Records Analysis

Activities that generate documents and records

- List the general types of activities within your organisation's functions that result in the production of documents or records.
- Identify the records creators.

Documents and records resulting from activities

- List the main types of documents and records resulting from these activities.

Existence of a records management program

- Describe activities currently undertaken that relate to records management.
- Analyze any policies that the creator might have that govern the creation and management of records.

Individuals responsible for records maintenance

- Identify the individuals(s) responsible for keeping the records after their creation (records maintenance). This might be designated records personnel, or may be the creators of the records, or both.

Existence of maintenance strategies

- Identify the complex of practical means, either formally articulated or informally implemented, that constitute the management of records. This includes:
  - The location in which the records are kept,
  - The medium/media in which records are kept,
  - A description of how records are organised,
  - A brief description of any methods used to maintain records,
  - A brief description of any methods used to attempt to avoid technological obsolescence while the records are still active or semi-active.

Technological Requirements and Constraints

- Identify and describe the equipment used in your organisation:
  - Architecture (e.g., network topology, infrastructure, hardware),
  - Creation or input tools (e.g., software, camera, microphone),
  - Processing tools (e.g., for example software, console).
- Identify and describe the types of media created (e.g., graphic, textual, audio).
- List the formats created (e.g., .pdf, .doc, .jpg) and identify any particular challenges related to their maintenance and preservation.
- Identify and describe how relevant technological requirements/constraints impact upon the creation, form, content, identity, integrity, organisation and preservation of the records.