

Storing Information in the Cloud – A Research Project

Kirsten Ferguson-Boucher and Nicole Convery

Cloud computing as a new delivery model is proving challenging for recordkeeping professionals. The ARA/Aberystwyth University research project, 'Storing Information in the Cloud' aimed to investigate the management, operational and technical issues surrounding the storage of information in the cloud. It also set out to develop a toolkit that could assist information professionals in assessing the risks and benefits of outsourcing information storage and processing. Based on the information gathered through a literature review, questionnaire, an unconference, as well as interviews with cloud providers and customers, the outcomes included the Cloud Computing Toolkit, a list of cloud computer resources relevant to the records and information community and specific recommendations. These include further research into the implications of cloud computing for record-keeping principles and practice and the development of cloud-specific guidance and policies and a pool of resources relating to cloud computing and information management. The extension of the research to consider its implication for the long-term preservation of digital material was also a recommendation and the development of a more active role for professional bodies in bringing together information professionals and in forming interest/working groups on specific related to cloud computing. New technologies or new models continue to challenge the profession's ability to maintain information governance and assurance and on-going research is required to ensure that we address the practical and strategic issues of the fluid information ecology.

Introduction

Social media tools and cloud computing are currently invading the corporate environment and have generated some debate amongst record-keeping professionals who have to be aware of the full implications of corporate assets being deployed into

Correspondence to: Kirsten Ferguson-Boucher, Lecturer in Records Management, Aberystwyth University, Llanbadarn Campus, Aberystwyth, Ceredigion SY23 3AS, UK. Email: knb@aber.ac.uk

the cloud. For many organizations, cloud computing presents an attractive model for delivering efficient IT services remotely. The use of web-based services and applications is becoming more widespread in both public and private sector organizations,¹ and many the so-called Web 2.0 trends are based on storage of information outside organizational server environments and firewalls.²

Little actual research has so far been undertaken to assess formally the impact of these new technologies on professional practice. The Archives and Records Association sought to commission some preliminary research into the implications for the records and information management (RIM) professions of storing information in the cloud and Aberystwyth University secured the funding.

The eight-month research project commenced in February 2010 and investigated the legal, technical and operational concerns regarding the storage of corporate assets in a virtual environment. It was envisaged that this introductory work would provide practitioners with a basis for a more structured discussion of the impact of cloud computing on RIM processes. The project also aimed to produce a toolkit that would provide practitioners with a framework, comprising key considerations and questions, to assist with setting up cloud computing environments.

This article will explore the emerging view of cloud computing in the context of this study. The sections will focus on the following:

- Context and methodology.
- Findings and outcomes.
- An overview of the challenges and drivers.
- The toolkit: a risk, governance and stakeholder perspective.
- Benefits and future research.

Some Context

Cloud computing can be described as the ability to access a pool of computing resources which are owned and maintained by a third party via the internet.³ It is not a new technology but a new way of delivering computing resources based on long existing technologies such as server virtualization.⁴ The 'cloud' as such is composed of hardware, storage, networks, interfaces and services that provide the means through which infrastructure, computing power, applications and services are accessed by the user on demand and independent of location. Cloud computing usually involves the transfer, storage and processing of information on the provider's infrastructure which is outside the control of the customer.

There is as yet no standard definition for cloud computing but the National Institute of Standards and Security (NIST) defines it as 'a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction'.⁵ NIST distinguishes

between three delivery models [Software-as-a-service (SaaS), Platform-as-a-service (PaaS) and Infrastructure-as-a-service (IaaS)] and four deployment models (public, private, hybrid and community clouds).

Cloud computing services make use of economies of scale in large server farms or data centres, which enable them to reduce the cost of using information technology resources through optimal resource utilization. Organizations can access these cheap computing resources via an internet connection on demand and on a pay-per-use basis without having to invest in their own IT infrastructure. But whilst this new business model is seen as revolutionizing the way organizations use and provision IT resources, cloud providers in the UK find that actual adoption of cloud services remains low compared with the US.⁶

Methodology

Literature Review

The first step of the research was to undertake a literature review. This revealed that few academic studies are available which focus on organizational or information management aspects of cloud computing. Even fewer studies concern themselves with the more specific relationship between cloud computing and RIM, exploring life-cycle management, compliance or risk management. In effect, the literature review provided a first indication of the fact that cloud computing is still in an early adoption stage in which technical concerns and product reviews dominate. Analyses of the state of cloud computing and the development of cloud standards and strategies are largely missing.

There is, however, a recent JISC study on cloud computing specifically for research which has produced two reports analysing cloud computing barriers and drivers and provided research-focussed case studies and technical specifications for cloud computing.⁷

Consultations

Online Questionnaire

The second stage of the methodology was the circulation of an online questionnaire, hosted by Bristol Online Surveys and conducted in March 2010. The questionnaire was distributed on a range of JISC lists including archives-nra, records-management-uk and lis-ukeig and was also retweeted on the microblogging service Twitter. It was advertised on the Department of Information Studies VLE (Moodle) and homepage. A total of 41 information professionals (archivists, librarians, records and information managers, IT managers) completed the questionnaire.⁸ Tables 1 and 2 present a breakdown of the individuals who responded to the questionnaire.

Table 1 Respondents by Sector (Convery 2010).









Which sector does your organisation operate in?			
Private sector		19.5%	8
Public sector		75.6%	31
Third/voluntary sector		4.9%	2

Table 2 Organisation Size (Convery 2010).

How many employees does your organisation have?			
Less than 100		17.1%	7
100–499		22.0%	9
500–999		7.3%	3
1000–1999		22.0%	9
over 2000		31.7%	13

Although this might appear to be a small number of respondents, the return is comparable to similar research projects such as the ENISA cloud survey which attracted 74 responses in a European-wide survey.⁹ The relatively low number of responses provides another indication that use of cloud computing and awareness of its associated benefits and challenges have yet to gain ground among the information professions.

Interviews

The online questionnaire was followed by more in-depth interviews with IT managers from two private sector organizations (Melrose PLC and Guardian News & Media) which have successfully implemented cloud computing services. A third interview was carried out with a representative from the Cabinet Office, concerning the G-Cloud, the government's private cloud initiative. The interviews informed the case studies made available in the report.¹⁰ It proved difficult to identify organizations which had implemented cloud computing solutions, again an indication of the embryonic stage reached in the records and information community.

A range of cloud service providers were interviewed either in person or over the telephone to discuss their services, security measures and pricing models.¹¹

Events

The project team organized an 'unconference' on 21 May 2010 in which 30 people from a wide range of professional backgrounds, including archivists, records

managers and IT managers, participated. The workshop-based, participant-driven unconference format was chosen over more traditional conference formats. It was felt that an unstructured, facilitated environment would encourage an open exchange of experiences, concerns and solutions to managing information stored in the cloud. As cloud computing is still an emerging field and not many professionals have practical experience in outsourcing to the cloud, an explorative event was felt to be adequate for fostering debate on the topic. The organizers diverted from the completely open, unstructured unconference format by providing three expert speakers (Dai Davies, Paul Miller and Steve Bailey). Each gave a 20-min overview of particular cloud computing concerns (information security, compliance and records management) and then facilitated the following discussions among participants. The rationale for the addition of some minimal content and structure was informed by the research that had been carried out to date. It became obvious from the earlier online questionnaire that many information professionals felt unsure about what exactly constituted cloud computing, and the event offered the opportunity to provide some clarification about the subject in general. The themed approaches, it was hoped, would encourage debate in the key areas identified in the literature review, the questionnaires and interviews.

Project Findings: An Overview of the Challenges and Drivers

From the consultations with members of the information management communities, it became clear that cloud computing was familiar to most as a 'new technology' that promises to save money, improve efficiencies and provide a 'greener' alternative to traditional computing. Many, however, felt that they lacked the necessary background knowledge to assess the usefulness and impact of cloud computing on their organizational environments. Widespread interest but low adoption can be explained with the status of cloud computing as an emerging business model that has yet to be sufficiently tested.

The concerns that emerged from the questionnaire are shown in Table 3.

Lack of trust has emerged as a main factor stalling the adoption of cloud computing. Information is perceived as an important business asset that needs to be protected, and outsourcing information storage to the cloud is often associated with a transfer of control over information security to the cloud provider. Therefore, cloud delivery models, such as private or community clouds, that provide a higher degree of control over the applications and infrastructure on which information is stored are preferred. It is expected that private cloud models will be adopted more widely in order to avoid information security risks associated with multi-tenancy and distributed data centres. Private cloud models utilize the existing infrastructure within an organization, optimised through server virtualization and centralization (Table 4).

Many of the information management practitioners consulted felt that the adoption of cloud computing was often *ad hoc* and driven in the main by IT

Table 3 Cloud Computing Challenges (Convery 2010).

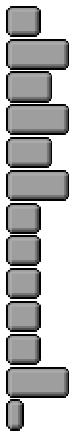

What are your main concerns regarding the use of cloud computing services?			
Compliance and e-discovery		n/a	14
Data protection (location of the data/server)		n/a	25
Integrity of data		n/a	17
Confidentiality of data/unauthorized access		n/a	24
Availability and reliability of services		n/a	19
Loss of control over data and services		n/a	26
Ability to audit service		n/a	16
Portability and interoperability of cloud services		n/a	13
Unknown cost due to variable pricing structure		n/a	13
Infrastructure and network security		n/a	14
Lack of customization/integration with existing systems		n/a	14
Retrieval and/or destruction of data when service terminated		n/a	29
Other (<i>please specify</i>)		n/a	4

Table 4 Cloud Computing Deployment Model (Convery 2010).

Which cloud computing deployment model do you currently use, are you planning to use or do you consider the most suitable for your organization?			
Public cloud		24.4%	10
Private cloud		36.6%	15
Community cloud		12.2%	5
Hybrid cloud		12.2%	5
Other (<i>please specify</i>)		14.6%	6

departments in response to changing business needs, shrinking budgets and overloaded IT systems. Few organizations utilized cloud services as part of a wider business strategy that also took into account information life-cycle management or solutions to long-term preservation needs. This is highlighted by questionnaire responses as shown in Table 5.

Most perceived cloud computing limited to IT implementations or as initial test beds for larger projects. It emerged as a frequent concern to information professionals that they are often not identified as stakeholders in IT projects and are not consulted prior to implementation. The lack of involvement of information professionals in many IT projects is not a new concern. When projects involve the storage of information in the cloud, however, new challenges to information security and compliance arise which can leave organizations in breach of laws and regulations.

Records management specific use cases

Cost and technical reasons are the main drivers given by information professionals for cloud computing adoption and indicate a very IT-centric view of cloud computing.

Table 6 shows what the questionnaire respondents identified as drivers for cloud computing.

Optimizing IT infrastructure and better flexibility and scalability are the next highest in the list of cited benefits of cloud computing. These tend to improve existing provisions of Information and Communications Technology (ICT) in organizations but do not necessarily improve actual business processes or indicate an appetite for systems and process innovation. More business-oriented and, therefore, more RIM specific drivers such as business process modernization, new application development and business continuity strategies are listed as benefits but do not rank as highly.

Cloud computing technologies appeal to organizations because they enable them to access cheap computing resources via the internet on demand and on a

Table 5 Use of Cloud Computing (Convery 2010).

Which of the following statements most closely represents your organization's use of cloud computing?			
We have used cloud computing for several years now		9.8%	4
We have used cloud computing for less than a year	=	19.5%	8
We are actively planning to use cloud computing in the near future		17.1%	7
We are interested in cloud computing but have not active plans yet		41.5%	17
Other (<i>please specify</i>)		12.2%	5

Table 6 Drivers for Cloud Computing (Convery 2010).

What are your organization's main drivers for cloud computing?			
Reduced ICT spending	=	n/a	27
Higher flexibility and scalability		n/a	25
Ease of use		n/a	12
Modernisation of business processes		n/a	12
Optimisation of IT infrastructure		n/a	20
Business continuity and disaster recovery		n/a	14
Access to applications not available in-house		n/a	15
Improved reliability		n/a	14
Other (<i>please specify</i>)		n/a	6

pay-per-use basis without having to invest in their own IT infrastructure or software applications. Cloud service providers offer a range of services from pure computing power and storage capacity to easily deployable business applications. Cloud computing services are often easy to set up and relatively commitment-free and, therefore, provide an attractive option to traditional ICT provisions. Main use cases for cloud computing as cited by the questionnaire respondents are information storage, the use of email and online office applications, and project management applications. Many of these applications involve the transfer, storage and processing of information on the cloud provider's infrastructure and therefore have a direct impact on organizations' record-keeping processes and policies.

Storing information in the cloud can range from simple storage and repository approaches for inactive records to applications that have document or even records management functionality similar to traditional in-house Electronic Document and Records Management Systems (EDRMS). Outsourcing information storage can free up internal computing resources, save cost and enable information management specialists to concentrate on the management of active, vital information.

Information storage also encompasses strategies for business continuity in the cloud where vital organizational information is replicated to cloud providers' infrastructure to be accessed in case of an emergency or systems failure. Rather than investing in expensive infrastructure onto which information can be redundantly replicated, which is never used to its full capacity, organizations can set up redundant information storage in the cloud often at much lower cost. Using services such as Amazon's Web Services (AWS) allows organizations to consume 100% of services and capacity to access replicated information on virtual servers when needed for business continuity, but incurs only minimal storage and maintenance cost when internal systems are running normally.

From the questionnaire as well as through attendance of various cloud-specific workshops and meetings across the public and private sector during 2009 and 2010, it became clear that many organizations are currently investigating the use of Software-as-a-Service (SaaS) models to save cost while still providing quality productivity applications to users such as email, word-processing and collaboration tools.¹² Outsourcing these services can save the cost of acquiring expensive licences for traditional products that often lock the organization into a particular product long term. They also allow out-of-hours, location-independent access to information for an increasingly mobile workforce. Cloud-based email applications such as Gmail are seen as more reliable than in-house applications and have a generous amount of email storage that is automatically redundantly backed-up. Email applications are often perceived as stand-alone, off-the-shelf products for which integration with other business applications such as an EDRM system has long been a challenge for organizations, but this fact appears to facilitate outsourcing to the cloud.

Collaboration tools in the cloud facilitate shared access to information, not just across organizational teams but with the organization's external partners and

customers. As collaboration tools such as project management applications and shared document repositories are not mission-critical applications and are not used frequently enough, organizations often do not want to invest in expensive software and licences. Cloud-based products have the advantage of being easily acquired, deployed and accessed when used as stand-alone products. Unfortunately, although these cloud-based applications can improve efficiencies, they can lead to an intensification of existing RIM problems. A distributed storage environment and potential duplication of material in a variety of proprietary formats can make it difficult to apply general information management processes.

On a larger scale, public sector cloud computing initiatives are driven by government in the UK. The G-Cloud is part of the UK government's ICT strategy which aims to improve efficiencies and cut costs through the standardization and consolidation of infrastructure and capabilities, and the adoption and promotion of common standards.¹³ The government is looking to develop a private government cloud computing infrastructure with three strands: a private government cloud, data centre consolidation and an application store. Applications in the store will be commissioned from third-party developers and offered at best price to public sector bodies. The G-Cloud will be compliant with a set of selected, existing standards and built on the government's own existing infrastructure which ensures that some security risks, such as multi-tenancy and data centre locations, can be avoided. The promotion of these still-to-be-selected standards and the development of common cloud architectures will further consolidate and standardize the cloud computing market and will provide assurance to both public and private sectors.

The Challenges for Information Professionals

Apart from the relatively familiar challenges to organizations arising from the outsourcing of IT operations, cloud computing raises issues because of the specific way in which these services are offered, acquired, provisioned, used and terminated. The main challenges extracted from the literature review are the more technical issues such as infrastructure and network security, availability and interoperability. The information professionals consulted, not unexpectedly, cited

- information retrieval and destruction,
- loss of control over information and
- data protection

as the main obstacles to be overcome (see Table 3). Again, many of the issues raised with cloud computing are not new for information professionals. Storage of information in the cloud merely adds to the complexities that many professionals face when managing information across the organization's systems and infrastructure. These include those that focus on information management, such as

information life-cycle management, application of retention decisions and the ability to prove information authenticity, reliability and integrity, which are significant issues for information management in general.

Retrieval and destruction of information encompasses a range of challenges relating to how information can be identified, searched and destroyed once it has been stored in the cloud. The ability to attach and maintain metadata, as well as to apply retention decisions to information stored in the cloud, depends on the cloud service's systems functionality. It can be assumed that many popular SaaS products do not provide such functionality. Cloud providers' deletion practices are often based on the deletion of nodes that point to information in virtual instances. Eventual overwriting of the information on physical hard drives needs to be assessed to determine whether practices fulfil compliance requirements. Similarly, an exit strategy for the retrieval or destruction of the information stored in the cloud needs to be in place. Information retrieval can be difficult, time-consuming and costly if the cloud provider does not offer standard mechanisms for information retrieval. Transfer of information between different cloud providers can also be difficult, as cloud providers use proprietary application programming interfaces (API) and interoperability is widely lacking.

Loss of control over information stored in the cloud is a not only a concern with implications for the ability to manage the information life-cycle but also for information security and authenticity. Responsibilities for infrastructure, and thus information security, are to varying extents transferred to the cloud services' provider and need to be established from the outset. The ability to monitor and audit the cloud provider's systems is often restricted as cloud providers aim to keep details of their infrastructure and security processes secret from the competition and hackers. Failure to obtain access logs and incident reports from cloud providers can have an impact on the evidential value of information stored in the cloud for legal and compliance requirements. Lack of standards and audit procedures makes it difficult for the organization to obtain the relevant information to satisfy their compliance and 'due diligence' requirements.

Compliance with the Data Protection Act 1998 is a major concern for many information professionals when contemplating cloud computing services. Compliance with the Act is dependent on at least the ability

- to determine where information is physically stored on the provider's distributed infrastructure which is often situated in data centres around the world;
- to demonstrate that appropriate technical and organizational measures are in place to protect personal information from unauthorized access – responsibility for which will often have been transferred to the cloud provider;
- to ensure that personal information is not kept longer than necessary and
- to produce relevant personal information within set time limits in response to data access requests.

However, most cloud providers have recently changed their terms and conditions to specify the physical location of information stored in the cloud and often have or are seeking compliance to standards such as the Federal Information Security Management Act (FISMA) of 2002 and ISO27001 (Information Security Management) to prove their security credentials.¹⁴

Significant information security and compliance concerns regarding the storage of information in the cloud became evident during the consultation process. It can, therefore, be expected that in the near future mainly non-mission-critical applications storing non-confidential information will be selected for outsourcing to the cloud until the cloud computing market has matured and relevant standards and legislation are in place to ensure information security and compliance.

The Toolkit: A Risk, Governance and Stakeholder Perspective

It is clear from the findings that many of the concerns associated with cloud computing relate specifically to information governance, i.e. the handling of data in the cloud. Since information is a core business asset, it requires protection in the same way as every other asset, and the control of processes and procedures is equally important in a cloud environment. Decisions must be taken after consideration of the wider context of organizational strategy. They form part of a complex structure of assessments regarding information *value, alignment, performance* and *assurance*. All of these operate within an overarching risk framework. There are different concerns when *preparing* to use cloud computing services, to those most relevant when *managing* and ultimately *operating* in the cloud.

Methods of Assessment

Value

Information adds value when consideration is given to its classification, appraisal, access and preservation. In any information asset management decision, certain factors are essential to extracting the maximum benefit from the information content, ensuring that only the important information is retained, that it can be retrieved in the timescales required for business need, and that it is secure and yet accessible to all those who require it for as long as they require it.

Alignment and performance

Equally, information strategies are most successful when linked with the wider organizational initiatives on legal, structural, systems and operational levels, and mechanisms are in place to monitor their performance. The effectiveness, efficiency, flexibility and sufficiency of the solutions require consideration at planning as well as review stages of the procurement and operational process.

Assurance

For information professionals particularly, information assurance is a critical element of the decision-making process: the authenticity, reliability, availability, confidentiality and integrity of information require particular treatment. Vendors are increasingly expected to provide evidence of compliance with best practice recommendations. The research identified a Top 10 of Cloud Computing Concerns. These cluster loosely into those attendant with performance, specifically efficiency and cost, monitoring and total costs; those relating to alignment with organizational objectives, i.e. organizational responsibility and the impact of outsourcing; those associated with ensuring information assurance and value through Records and Information Management (RIM) programmes and the protection of systems. The perceived risk to the organization and the robustness of the contracts and outsourcing procedures were most significant to those questioned.

The Risk Framework

Risk management is essentially achieving a balance between the risk probability and impact, on the one hand and the sufficiency of the mitigation strategies and the impact they will have, on the other hand.¹⁵ When giving consideration to the various methods of assessment, identification and documentation of the risks and a mechanism for measurement will facilitate balanced approach to the decision-making process. Risk registers or logs provide a framework for identification and documentation. Whilst it is beyond the scope of this research to make specific recommendations as to the best method for managing risk, there are many existing frameworks which would lend themselves to this sort of analysis, measuring both the probability/impact and the mitigation sufficiency/impact.¹⁶ Time spent in the planning stages of the risk analysis will not prevent problems later in the operational cycle but will go some way towards ensuring that strategies are in place for the mitigation of those identified, should they be considered a sufficiently high risk category.

Risk management

Consensus emerged from the various consultations that the decision to use cloud computing can be seen as essentially a risk assessment and management exercise that should be familiar from other outsourcing projects. When outsourcing to the cloud, the organization transfers much of the control over computing resources, services and information to the cloud service provider. However, the organization remains responsible for the security and management of these resources and needs to assess what risks are associated with outsourcing to the cloud. Risk assessment needs to include compliance as well as RIM aspects. The technical aspects of the provider's IT infrastructure appear to be the main focus in current professional literature on cloud computing.

Risk assessment also needs to include a wide range of stakeholders: IT professionals, legal and compliance experts, procurement managers, records and information managers, archivists and digital preservation experts, business process managers and users. Records and information professionals are often not part of the cloud computing consultation processes or project team from the outset. Contributions from information professionals in the consultation process are either not valued or not evident to the organization. There is a widespread concern, therefore, that RIM-related risks are overlooked when organizations make the move to the cloud.

Risks, as identified by the literature review and the primary data collection, mainly fall into two categories: management risks (including information lifecycle management, compliance, contracts and cost) and operational risks (including security, access and business continuity risks). An organization's risk framework and appetite generally determine which cloud services and deployment models can be selected when outsourcing information storage to the cloud. For example, private clouds are deemed safer but may offer less flexibility and scalability, whereas SaaS transfers most responsibilities for information security to the provider, etc. Cloud computing invariably generates new risks, many of which can be transferred to the provider or mitigated through audit and monitoring of the provider's services and infrastructure. Other risks might have to be accepted as part of a trust relationship that is being established with a cloud service provider. Security and monitoring risks that occur where cloud providers either do not provide sufficient transparency or the relevant tools can be mitigated by third-party cloud services that specialize in offering value-added services such as Cloudreach. As one unconference participant puts it: 'You can have security in the cloud, it is just more expensive'.

The Toolkit provides guidance on how to approach the cloud as a storage solution, within this risk and governance framework and is divided into three sections: preparing, managing and operating in the cloud.

Preparing for the Cloud

The initial deliberations focus on alignment with business objectives. This encompasses alignment with

- the legal framework in which organizations operate;
- the existing internal systems for staff and other resources;
- the IT infrastructure and
- central business drivers and current initiatives.

These are obviously different for each organization, and successfully identifying the appropriate processes and models in the cloud is dependent on alignment in each of these areas. It is also dependent on the effective anticipation of the related risks and the identification of mitigation strategies.

The second consideration relates to the value-added elements that information can bring to the organization: identification of the information to be serviced in the cloud and some form of classification to enable its retrieval and effective usage.

Finally, risk analysis and assessment relating to the identification, analysis and development of responses to the security and governance risk. Stakeholders in this process include the owners of the business process or information asset that is to be moved to the cloud, the prospective users, and the project and risk managers who assess the overall risk of outsourcing as well, as the cost/benefit ratio. Records and information managers, who will have responsibility for managing information stored in the cloud, need to be involved from the outset, as well as the IT professionals, responsible for setting up and maintaining the cloud service.¹⁷

Managing the Cloud

If the planning stages are more concerned with the alignment, value and risk to the organization, the management of the information once in the cloud focusses more closely on the assurance and performance aspects of information governance. In order to manage information in this environment, particular consideration needs to be given to the characteristics of that information that ensures it continues to be of use to the organization. Some form of guarantee relating to the continuing authenticity, reliability and integrity of the information (terms which resonate for both the records and assurance industries) is required, dictated by legal and regulatory compliance. Service providers are increasingly under pressure to provide sufficient evidence of undertaking and monitoring the activities that ensure these are maintained. The contracts and service agreements are the documents which embody these understandings and support the specific nature of these arrangements.

The cost of using cloud computing is a significant consideration when managing the data in this environment. Cost/benefit analyses and indeed the wider performance measurements which can be used to assess how effective, efficient, flexible and therefore sufficient the cloud solution is proving necessitate constant monitoring. They also require a clear exit strategy, so that if cloud computing ceases to be the most suitable option as identified through any of the above assessments, a relatively painless and risk-free migration can be achieved. Indeed, all the considerations specific to the management of data in the cloud are best approached using a risk framework. In some instances, it may be that it is determined worth the risk or that the mitigation strategy for the risk that has been identified is considered sufficient to address identified issues. By continually reassessing and reapplying the risk criteria, across the spectrum of information governance concerns, a balanced approach to cloud usage is achievable.

If all stakeholders involved recognize their responsibilities and comply with policies and procedures set up for governance in the cloud, organizations can manage their cloud usage effectively. Stakeholders include the owners of the assets and the

RIM professionals, but also the archivists and digital preservation specialists, whose responsibility it is to ensure the information is available for as long as is required. Legal and compliance experts will need to assess the risks to maintaining the necessary record characteristics and the strategies and contracts employed.

Operating in the Cloud

Information governance issues relating to information assurance and information value are more pertinent in the operating environment. Stakeholders in these activities include the RIM, project, risk and IT professionals: those experts in the information and infrastructure security who will have been involved in any internal certification process. Information assurance and security considerations, such as assessing policies and procedures for physical, personnel, infrastructure, information and access security, require the involvement of cross-disciplinary teams and clear delineation of responsibilities between provider and customer.

The availability of the service is crucial, as are establishing adequate service levels and ensuring that the benefits offered by cloud computing such as rapid scaling of services are readily achievable. If breaches do occur, measurement and communication of the response times and effective mechanisms for minimising the impact and restoring systems form part of the strategy and understanding the resource provisioning employed by the provider.

In addition to issues relating to security, i.e. the withholding of access and availability of the services, the value of information is enhanced by provision of appropriate access to it. Access and identity management should embrace both security and access and ensure commensurate procedures exist in the cloud, thereby guaranteeing appropriate access to assets. Authentication, authorization and auditing of these procedures should go some way to evidencing the provenance of the information at a later date.

Finally, business continuity and the continuing access to information despite interruptions and failures at any stage of the life-cycle provide the final piece in the assurance jigsaw. Information Assurance principles are very similar to those of RiM: authentication, integrity, availability and confidentiality. Combined approaches to governance and assurance challenges should ensure robust and comprehensive solutions.

Benefits and Challenges

The research project set out to identify key legal, technological and organizational issues related to storing corporate assets in a virtual environment. It has provided an overview of cloud computing, storage and security literature and standards, and of cloud computing services and technologies to assist professionals in selecting the right provider. Based on the research, initial requirements for cloud storage that satisfy information governance and

assurance criteria have been proposed, and a toolkit applicable to all record-keeping professionals in their organizational context published.

Outcomes of the research are an extensive list of selected cloud computing resources relevant to the RIM community (<https://docs.google.com/Doc?docid=0AUMD4SCCG7uaZGRxczNybnfMTZjODM4bXhmNw&hl=en>) and bookmarked online resources (<http://www.delicious.com/nicoleschu/soacloud>).

The ongoing development of good practice guidelines requires dialogue between the wider stakeholder communities, the sharing of good practice as it emerges and a balanced approach to information governance and assurance. The research has provided an overview of current perceptions, availability and use of cloud services, and the opportunity to discuss the impacts and challenges of the cloud in international contexts. Meeting these challenges is not dissimilar to meeting the challenges presented by any other change in the information working practice of organizations. Information governance and assurance requires a balanced approach to each decision on the basis of risk to the organization. Established skills of information professionals are in demand to assist the specialist stakeholders in this cross-disciplinary and strategic approach. Risk management is perhaps not considered a core skill for RIM professionals but does form part of this existing skill set; judgements relating to storage, security and access in addition to appraisal and disposal are all decisions made within a risk context. To paraphrase from *New Skills for a Digital Era* (2008), information professionals need

- (1) familiarity with technology in their holdings (internal or external to the organization),
- (2) the ability to use the technology to do their jobs more effectively,
- (3) to be able to communicate with other communities,
- (4) to undertake cost-benefit analyses,
- (5) to undertake the administration, project management and evaluation of the digital collections in their care,
- (6) to manage the process and expectations and
- (7) to possess basic programming and systems skill to enable the above.¹⁸

Perhaps a skill that should be added to this listing is that of managing risk.

Future Research

What emerged from this investigation is that little research has been undertaken formally to assess the impact of cloud computing on professional information management practice. This is a concern for research universities, as well as for public and private sector organizations. A research collaboration has begun between Aberystwyth University and the Center for Information Assurance and Cybersecurity at the University of Washington, Seattle, USA to extend the Toolkit to an Information Governance and Assurance approach to the collection and use of

research data in the cloud. The objectives are based on the findings of the ARA-funded project and include exploration of:

- implications for record-keeping principles and practice;
- implications for long-term preservation of digital material;
- development of models for engaging professional bodies into a more active role;
- development of education artefacts for incorporation in information science curricula;
- enhancement of Toolkit guidance and standards.

We have long spoken about life-cycles, but what is evolving is perhaps more an 'information ecosystem'.¹⁹ In Thomas Davenport's visualisation, this represents a localised group of interdependent organisms together with the environment that they inhabit and depend on. Each is responsible for transforming its ecosystem and in need of an understanding of it and its interdependencies. Cloud computing forms a further component in the record-keeping environment. Further research is required into its nature, as we progress from the early stages of adoption, and into the interdependencies, particularly the challenges of ensuring that the data, wherever it resides, form part of the wider governance and assurance strategy.

Notes

- [1] See, for example, the case studies in Convery, *Storing Information in the Cloud – Project Report*.
- [2] Reese, *Cloud Application Architectures*.
- [3] Ibid.
- [4] ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.
- [5] NIST, *Definition of Cloud Computing*.
- [6] Preez, *Cloud Expo: Europe is 12 Months Behind the US in Cloud Uptake*, ENISA, *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.
- [7] See ENISA, *Cloud Computing Information Assurance Framework and Cloud Computing: Benefits, Risks and Recommendations for Information Security* Australasian Digital Recordkeeping Initiative, *Advice on Managing the Record-keeping Risks Associated with Cloud Computing*, and Hammond, *Cloud Computing for Research: Final Report*.
- [8] Results of the survey and information about sector and geographical spread are available from the project report (Convery, *Storing Information in the Cloud – Project Report*).
- [9] ENISA, *An SME Perspective on Cloud Computing*.
- [10] Convery, *Storing Information in the Cloud – Project Report* and *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*.
- [11] The list of cloud providers interviewed are listed in the Cloud Computing Report (Convery, *Storing Information in the Cloud – Project Report*).
- [12] For questionnaire results please refer to Convery, *Storing Information in the Cloud – Project Report*.
- [13] Cabinet Office, *Government ICT Strategy: Smarter, Cheaper, Greener*, Bellamy and Gallagher, *Data Centre Strategy, G-Cloud & Government Applications Store Programme Phase 2 Scope Report*.

- [14] BSI, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, United States Congress, *Federal Information Security Management Act 2002*.
- [15] IRM, *A Risk Management Standard*.
- [16] OGC, *Managing Successful Projects with PRINCE 2 and JISC InfoNet, Risk Management Infokit*.
- [17] TNA, *Managing Information Risk: A Guide for Accounting Officers, Board members and Senior Information Risk Owners*.
- [18] Pearce-Moses and Davies, 'New Skills for a Digital Era'.
- [19] Davenport, *Information Ecology: Mastering the Information and Knowledge Environment*.

References

- Australasian Digital Recordkeeping Initiative. 'Advice on Managing the Record-keeping Risks Associated with Cloud Computing. Draft v0.1.', 2010, <http://www.adri.gov.au/wiki/GetFile.aspx?File=ADRI%20statement%20re%20cloud%20computing%20v2.pdf> [accessed 4 October 2011].
- Bellamy, M. and G. Gallagher. *Data Centre Strategy, G-Cloud & Government Applications Store Programme Phase 2 Scope Report. Draft*. London: Cabinet Office, 2010.
- British Standards Institution (BSI). *Information Technology – Security Techniques – Information Security Management Systems – Requirements. BS ISO/IEC 27001:2005*. London: BSI, 2005.
- Cabinet Office. *Government ICT Strategy: Smarter, Cheaper, Greener*. London: HMSO, 2010, http://webarchive.nationalarchives.gov.uk/+http://www.cabinetoffice.gov.uk/media/317444/ict_strategy4.pdf [accessed 7 October 2011].
- Convery, N. *Storing Information in the Cloud – Project Report*. London: ARA, 2010, http://www.archives.org.uk/images/documents/Cloud_computing_report_final-1.pdf [accessed 4 October 2011].
- . *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*. London: ARA, 2010a, http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf [accessed 4 October 2011].
- Davenport, T. *Information Ecology: Mastering the Information and Knowledge Environment*. Oxford: Oxford University Press, 1997.
- ENISA. 'Cloud Computing Information Assurance Framework,' 2009, <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework> [accessed 7 October 2011]
- . 'Cloud Computing: Benefits, Risks and Recommendations for Information Security,' 2009a, <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment> [accessed 4 October 2011].
- . 'An SME Perspective on Cloud Computing,' 2009b, <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey/?searchterm=cloud%20computing> [accessed 4 October 2011].
- Hammond, M. *et al.* 'Cloud Computing for Research: Final Report. JISC', 2010, <http://www.jisc.ac.uk/whatwedo/programmes/researchinfrastructure/usingcloudcomp.aspx#downloads> [accessed 4 October 2011].
- Institute of Risk Management (IRM). *A Risk Management Standard*. London: IRM, 2002, http://www.theirm.org/publications/documents/ARMS_2002_IRM.pdf [accessed 4 October 2011].
- JISC infoNet. 'Risk Management Infokit,' 2009, <http://www.jiscinfonet.ac.uk/InfoKits/risk-management> [accessed 4 October 2011].
- National Institute for Standards and Technology (NIST). 'Definition of Cloud Computing. v.15,' 2010, <http://csrc.nist.gov/groups/SNS/cloud-computing/> [accessed 4 October 2011].

- Office for Government Commerce (OGC). *Managing Successful Projects with PRINCE 2*. London: HMSO, 2006.
- Pearce-Moses, R. and S. Davis, ed. 'New Skills for a Digital Era'. Conference Proceedings. Society of American Archivists <http://www.archivists.org/publications/proceedings/NewSkillsForADigitalEra.pdf> [accessed 4 October 2011].
- Preez, D. 'Cloud Expo: Europe is 12 Months Behind the US in Cloud Uptake,' 2011, Computing.co.uk, <http://www.computing.co.uk/ctg/news/2024048/cloud-expo-europe-months-cloud-uptake> [accessed 3 February 2011].
- Reese, G. *Cloud Application Architectures*. Sebastopol, CA: O'Reilly Media, Inc, 2009.
- The National Archive (TNA). 'Managing Information Risk: A Guide for Accounting Officers, Board members and Senior Information Risk Owners', 2008, <http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf> [accessed 7 October 2011].
- United States Congress. Federal Information Security Management Act 2002, 2002, <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> [accessed 4 October 2011].

Copyright of Journal of the Society of Archivists is the property of Routledge and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.