ESARBICA JOURNAL

JOURNAL OF THE EASTERN

AND SOUTHERN AFRICA

REGIONAL BRANCH OF THE

INTERNATIONAL COUNCIL ON

ARCHIVES

Volume 37

2018

ISSN 2220-6442 (Print), ISSN 2220-6450 (Online)

RISKS ASSOCIATED WITH CLOUD COMPUTING IN PURSUIT OF EFFECTIVE RECORDS MANAGEMENT

Cameron Bassett
Commonwealth Bank of Australia
cameron@cameronbassett.com

Isabel Schellnack-Kelly
Department of Information Science
University of South Africa
schelis@unisa.ac.za

Received: 20 May 2017
Revised: 3 May 2018
Accepted: 10 August 2018

Abstract

Using literature review, this article examines the risks associated with cloud computing and how cloud computing could be considered when implementing effective records management in the public sector. The discussion in this article has been facilitated by an extensive literature review related to cloud computing, records management and technology concerning governance and accountability. The article also discusses the risks that public entities need to bear in mind when considering cloud computing as a solution to implementing effective records management controls and practices. The article discusses how cloud computing can benefit organisations. Cloud computing has many advantages but there are also risks that are associated with it and these are mentioned in the article.

Keywords: cloud computing, governance, compliance, enterprise risk management, local government

Introduction

Cloud computing has arisen from harnessing the power of the internet by ensuring that data and documentation can be accessible anywhere and at any time. The capabilities of cloud computing create new records management possibilities by ensuring that documentation can be accessed from any location and at any time. Access to information is critically important to public entities as evidence of governance, transparency, accountability and ensuring effective service delivery. The South African local government sector is such a case study. The reports from the Auditor-General of South Africa year on year indicate that records of local governments cannot be found and this has repercussions, resulting in poor service delivery and development planning initiatives. The focus of this article was to examine the risks of cloud computing and the possibilities of cloud computing to ensure effective records management in South Africa's local

government sector. Problematic records management is a feature of South Africa's local government sector. Using literature, this article discusses how cloud computing, records management and technology can aid governance and accountability.

Literature review

Records management and technology in the interest of governance, transparency and accountability

The general literature relating to this theme is from scholars such as Cox (2005, 2006), Dryden (2010), Hunter (2004), Hurley (2004), McKemmish (2001), Mnjama and Wamukoya (2007), Shepherd (2006), Stearns (2010), and Wallace and Webber (2011). Meanwhile, literature from South African and African scholars, such as Katuu (2012), Makhura (2009) and Ngoepe (2008; 2012) concerning discussions related to the creation, management and preservation of all records in electronic or digital format were consulted.

The 21st century began with two events that catapulted the significance of records linked to transparency, accountability and security, and subsequently, governance. First was the collapse of Enron, a United States multinational corporation, which "shook the corporate world around the globe" (Isa 2009:233). The purposefully shredding of supporting documents and Enron accounts to conceal improprieties and the generation of fake records demonstrating accountability reveal the failure of accountability processes (Isa 2009:233). Boards of directors are accountable for actions and business operations and should not declare their unawareness of wrong doings by their subordinates (Isa 2009:63). This event required records management to become a boardroom conundrum. The other event catapulting the significance of records management was the terror attacks in United States in September 2001. The complete destruction of paper-based records of the 1 200 businesses destroyed in the World Trade Centre Towers provided incentives for increased emphasis on converting official records and strategically vital records to digital format, with disaster management and off-site back-up strategies (Stephens 2003:34-39).

Democracy and governance touch on the fundamental right of citizens and this includes accountability of the government to the governed (Petlane & Gruzd 2011:19). These fundamentals have widened the selection of auditors and auditing processes to include financial reporting standards, strengthening internal managerial controls, monitoring compensation

standards, observing cyber security and technology standards (Bhimani 2008:135-137). All of these standards, codes and practices should apply to the South African local government sector.

Additionally, the role of this public sector in appointing and supporting information management requires comprehensive understanding of the dynamics associated with creating, managing and disposing of information sources. Better attention to accuracy, proficiency and more customer-driven solutions, forming the benchmarks of creating and managing the information sources, would enable local governments to vastly improve public perceptions (Ketelaar 1992:5-6). The subsequent spinoff of local government having accurate, available information for decisions, planning and executing sustainable development initiatives, settling legal disputes and providing factual accounts to auditors concerning the utilisation of taxes and funds, would boost South Africa's persona, both within the country and on the international stage. Cloud computing could provide a platform to ensure that documentation is securely captured and available whenever required for governance and operational purposes.

Understanding cloud computing

There is a multitude of definitions of what "cloud computing" is and many of these are conflicting. It is either defined by a very narrow definition, where cloud computing is seen as "utility computing" or a broader, umbrella definition which encompasses everything that is related to virtual computing (Rittinghouse & Ransome 2010:xxvii; Bassett 2015:32). Bassett (2015) defines cloud computing as a multi-tenancy system of hard and soft virtualised resources with utility properties. These rapid, on-the-go, adjustable pooled resources are used as an alternative to onsite storage applications and provide virtual computing services, wherever an internet connection is present (Bassett 2015:38).

Cloud computing is based on the idea of pooling physical resources (e.g. systems and storage) and presenting them in a virtual form (Sosinsky 2011:25). Virtualisation refers to the simulation of IT resources on a physical host server (Himmel 2012:125). Virtualisation gives applications the ability to be transferred to other hardware images, without alerting the application to this movement. These applications are "virtualised" when they are isolated from the hardware in this manner (Himmel 2012:21). Cloud computing has many risks. For the purpose of this paper, a risk has been defined by Bassett (2015:70) as "the threat, or danger that the use of cloud computing can pose to tasks or situations, which might test the abilities of cloud computing by

presenting difficulties in allowing for success to be achieved (such as what needs to be overcome to allow cloud computing to prove or justify itself)".

Records management, technology and governance

In an article by Asogwan (2012), electronic records management has transformed the traditional models of record keeping and requires records managers and archivists to remain relevant by seeking relevant solutions in the information society. Asogwan (2012) has shown that there are major problems with the e-records management in Africa. Technical and administrative challenges have been introduced and require managing hybrid records. Appropriate infrastructure, legislation, regulatory frameworks, finance and staff competent in ICT are required to address the risks, as well as the benefits of ICT solutions, such as cloud computing as a method to resolve storing records, saving costs of staff and ICT hardware (Asogwan 2012:198).

Risks associated with cloud computing

Bassett (2015:78) identifies 10 risks associated with cloud computing. These are: compliance; legality and auditability; security; everywhere accessible data; incident response, notification and remediation; virtualisation; governance and enterprise risk management; interoperability, portability and data lock-in; viability; and availability and reliability. Each of these risks is explained hereunder.

Compliance: The Cloud Security Alliance (2011:46) defines compliance as the awareness of and adherence to obligations (e.g. corporate social responsibility, applicable laws and ethical guidelines), including the assessment and prioritisation of corrective actions deemed necessary and appropriate. Compliance is a significant challenge for cloud computing, pre-existing compliance as well as information security standards which may not be applicable, as they were not originally designed with cloud computing in mind. An example provided by Convery (2010:13) illustrates this in the case where the owner of data may need to identify the physical location of the data being stored. However, when the data resides on a multi-tenant system, this may not be possible, as this would cause a failure to achieve any certification of compliance.

If an organisation is considering utilising an overseas cloud service provider, they would need to be aware of the regulation requirements and legislation pertaining to that specific geographical area. The types of information that are being stored in the cloud would also impact on

compliance issues (Queensland Government 2013a). An example of this is in the case of the United Kingdom. With regard to the Data Protection Act, 1998, which requires restriction pertaining to personal information to not be transferred to a country that is not a part of the European Economic Union, unless the country is able to provide an acceptable level of protection for the individual's freedom and rights when the personal data are processed (ICO n.d:9).

Legality and auditability: These refer to an organisation's compliance in operating in accordance with the law and, if inspected, in being held accountable. Organisations need to comply legally with acts and regulations in their home country. However, with cloud computing, data can be hosted offshore in various geographic locations and jurisdictions. This creates legal implications requiring consideration, as data hosted in those countries are subject to the legislation pertaining to those countries. Hosting laws and service level agreements can compromise the advantages of cloud computing. The challenge of the hosting laws is explained to enhance clarity. A unique feature of cloud computing is its data hosting, which can be based in various locations worldwide (Heiser & Nicolett 2008:3; Thomas 2010:219). However, information that is hosted in the cloud is subject to the jurisdiction of the country where the data are being hosted physically. This could present a problem, as illustrated in the following example. Due to cloud computing utilising a multi-tenant system, a drive may be shared with other clients. If a drive is seized by law enforcement, many of the clients will not be able to access their information (Convery 2010:13; Gellman 2009:5). This could impede daily business operations, which contests cloud computing's viability for records management.

Cloud computing can significantly affect information privacy and confidentiality. Where information is being hosted by a third party, the cloud service provider may be hosted offshore. This service provider may transport the information over other geographic boundaries, which could in turn be affected by the regulatory and legal requirements of the stored information (Antonopoulos & Gillam 2010:276). An example of jurisdictional law of a country where the data are being hosted is that of the United States of America. Data hosted in the United States are subject to the US Patriot Act of 2001, Public Law 107–56 (Cervone 2010:165). In accordance with this piece of legislation, information stored in the cloud of a company falling within the jurisdiction of the United States may be opened for access by external forces.

The cloud service provider should provide a minimum service level to the client (Antonopoulos & Gillam 2010:253). The service level agreement (SLA) needs to be specific to ensure privacy and compliance. For example, if another cloud client is undergoing audit proceedings, the cloud service needs to be able to ensure the privacy of other clients utilising the same drive for their data storage (Himmel 2012:109). Furthermore, Himmel (2012:109) states that this agreement must include stipulations for data location, data management, backups and how the service provider can assist in auditing.

In essence, legal compliance and auditability refer to the user's accountability for the integrity and security of its data, even when they utilise a service provider. Traditional service providers participate in external security certifications and audits. A cloud computing service provider should be able to provide their client with this information for their clients' audit purposes. If they are unable or unwilling to do so, they are indicating that their services are only applicable for basic functions and services (Heiser & Nicolett 2008:3). Furthermore, they may be unwilling to provide this information, as they may not be adhering to the law. A pre-existing industry standard can be affected by organisations moving their data to a cloud environment, as many standards were not created with cloud computing in mind (Convery 2010:35). For example, a standard such as ISO27001 or ISO9000 may require that the owner of the information be able to show the physical location of the stored information.

Industry regulations and regional laws can be complicated and often overlap (Antonopoulos & Gillam 2010:244). This is demonstrated by an example from the United Kingdom, where the Freedom of Information Act of 2000, the Environmental Information Regulations of 2004 and the Data Protection Act of 1998 require public sector organisations to make selective information available to the public within a certain period of time. Organisations that do not conform may be subjected to financial penalties as well as legal action through the Information Commissioner's Office (Convery 2010:34).

The term eDiscovery refers to the procurement of any electronic data for its use as evidence in a legal case (Biggs & Vidalis 2009:2). Organisations need to be able to provide access to electronic information for legal purposes, such as litigation (Convery 2010:35). The hosting location of cloud data is an area that needs careful attention with regard to such factors as compliance, auditability and eDiscovery (Cervone 2010:165). An organisation needs to ensure that its records management system is extended to its cloud-based storage (Convery 2010:35). However, an

organisation needs to have the same amount of control over its information in the cloud, such as identification, retrieval and halting destruction of information as they would in a traditional storage system (Convery 2010:35). There could be serious consequences if an organisation is unable to provide the necessary electronic data when required.

Security: This is perhaps the biggest risk faced by cloud computing. With cloud computing, the provider must ensure that client data are secure. However, it is the client's responsibility to ensure that the provider is able to provide the necessary security for their data. Data must remain secure, authentic, confidential and reliable (Convery 2010:13-14). Bassett (2015:85-95) identified specific risks related to security with regards to cloud computing. These are:

i. Identity authentication and access management
ii. Human factors
iii. Surface attacks and vulnerabilities
iv. Security as a service
v. Application security
vi. Traditional security
vii. Business continuity
viii. Disaster recovery
ix. Encryption and key management

Most of these challenges are not new to information technology and data security. Challenges like surface attacks such as viruses, Distributed Denial of Service (DDOS) attacks and Trojans, affect both in-house data storage as well as cloud-based storage (Opala 2012:47-52). However, these concentrated attacks increase the risk. This is attributed to the fact that many organisations are utilising cloud storage and these cloud storage centres have become targets for attack (Himmel 2012:108). Organisations need to evaluate their cloud service provider security to determine whether their data is secure. This can be aided by cloud computing service providers being transparent. One provider may not be a viable option for an organisation, while another provider may be (Bassett 2015:95).

Everywhere accessible data: The ability to gain access to data everywhere and anywhere has been referred by Bassett (2015) as "everywhere accessible data" and has discussed the risk in terms of mobile devices and collaboration tools. With the expansion of cloud computing use, more and more mobile devices, such as the cellular phones or tablets (i.e. iPad, Surface tablet etc.)

are being utilised for mobile access. These devices bring about their own security concerns, as they may not comply with security standards because the software is still immature and vulnerable (Himmel 2012:106-107).

Gartner (2013) predicts that at least 60% of information workers will utilise a content application through a mobile device. Risk arises when, due to the large increase in mobile solutions and productivity tools, organisations are being persuaded to migrate their data to the cloud. Often, there may not be sufficient security in place or issues relating to compliance (Buckley 2013). The issue of cloud computing's viability for records management can also be questioned. In a recent survey on mobile business users, conducted by the company Harmon.ie (Buckley 2013), it was found that 41% of mobile users admitted that they ignored company policies and stored and shared corporate documents on unapproved cloud services such as GoogleDocs and Dropbox. This could lead to serious issues related to confidentiality of secured data.

Document management collaboration tools are enhanced by cloud computing. However, in a study of the social collaboration habits of a thousand businesses and IT decision-makers, consulting firm Avanade found that a large majority of the users were using third-party tools, such as Facebook, instead of enterprise collaboration tools (Buckley 2013; Avanade 2013). This draws into question the security and privacy of what could be organisational intellectual property that is being shared and made accessible to anyone.

Incident response, notification and remediation: This risk not only relates to the fact that an incident occurred but, also the way in which it is handled that can pose a risk. An incident refers to an event occurring, which may have a positive or negative effect on the entity. If an incident is handled incorrectly or at a delayed pace, the damage it can cause could be increased. Clients who utilise cloud computing, in particular organisations, should be aware of how incidents are responded to by the cloud service provider. The service provider should notify the clients when there is an incident and inform them of how the incident is being remedied.

Although cloud computing does not require a new method of conducting an incident response to be developed, the organisation must adapt the existing incident response processes to include the new cloud environment (Cloud Security Alliance 2011:93). The incident response plan must be formalised and documented, outlining all the roles of those involved (Antonopoulos & Gillam 2010:253). There are characteristics of cloud computing that directly influence incident

response activities (Cloud Security Alliance 2011:93-94). They are on-demand-self-storage, rapid elasticity and resource pooling, and data crossing geographic boundaries.

According to Cloud Security Alliance (2011), cloud computing's on-demand-self-storage feature can make it difficult for a client to acquire the necessary support from their cloud service provider when a security incident needs attention. This may depend on the service provider's deployment and service model, where the actual scope of a service provider's incident detection, analysis, as well as their containment and recovery abilities may be dependent on the service level they provide (Cloud Security Alliance 2011:93-94). Meanwhile, rapid elasticity and resource pooling offered by cloud services may directly increase the difficulty of the incident response processes, particularly forensic activities that are conducted in conjunction with incident analysis. These activities need to be conducted in a highly dynamic environment that can challenge the essential forensic activities (such as the collection of data, devising scope of incident, preserving data integrity and stability). Due to cloud computing operating in a non-transparent environment, these problems are intensified when cloud clients endeavour to conduct forensic activities themselves, because the cloud service provider is unable to provide any support (Cloud Security Alliance 2011:94). Cloud computing can cause a client's data to cross a geographic or even jurisdictional boundary based on its data centre's location. This may occur without the client's knowledge. This, in turn, can cause the data to be impacted in incident response procedures due to legal limitations on what may, or may not be done, or what can, or cannot be done (Cloud Security Alliance 2011:94).

Incident remediation refers to how an incident can be remedied once it has occurred. Cloud computing, however, does create an advantage for incident response where the continual monitoring of the systems can reduce the amount of time to handle an incident response. Furthermore, due to virtualisation, the containment and recovery can be expedited with less interruption. The enquiry into an incident could be significantly easier in certain areas such as scenarios where virtual machines can be transported into a laboratory environment where forensic images are examined and an analysis conducted (Cloud Security Alliance 2011:94).

Virtualisation: Sosinsky (2011:25) refers to virtualisation with regard to cloud computing as a virtual, non-physical system, where resources are pooled together and shared. The cloud client is responsible for the security of the virtual machine. However, the cloud service provider is responsible for the secured virtual machine images (Bouayad et al. 2012:29). The Cloud Security Alliance (2011:157) identifies the following virtualisation risks: performance concerns; virtual machine guest hardening, inter virtual machine attacks and blind spots, operational complexity from virtual machine sprawl; virtual machine encryption; instant-on gaps; virtual machine (VM) data destruction; virtual machine image tampering; and in-motion virtual machines.

Hypervisor security and multi-tenancy systems in cloud computing are linked. The hypervisor refers to the software in-between the operating system, the hardware that is used to map resources between the system and the VM risk (Bouayad et al. 2012: 29; Himmel 2012:21, 26). Multi-tenancy is where resources are shared between VMs on a server, such as memory, CPU, storage, firewalls and even software services (Cloud Security Alliance 2011:64; Himmel 2012: 104). The hypervisor is used to create isolation between the VMs on the server. This is done to prevent cross-exploitation of isolated VMs which may be hosted on the same sever. Otherwise, users may be able to exploit these security vulnerabilities and obtain sensitive information from other VMs through shared resources (Cloud Security Alliance 2011:64; Himmel 2012:40, 104). This can draw into question privacy issues for users (Mollah, Islam & Islam 2012:4) and cloud computing's viability for records management, where restricted documents or records could be accessed by outside users. Unfortunately, if the hypervisor is no longer secure then all VMs are at risk (Bouayad et al. 2012: 29; Himmel 2012:21, 26). Clients may choose to utilise their own security configurations for their VMs. However, when they do not utilise the security controls of the cloud service provider, it can result in breaches in the security system. This can arise due to conflicts with the client's security configurations (Bouayad et al. 2012:30).

The rapid scalability of cloud computing is an advantage, especially with automation processes such as VM creation and backups. However, if there is a problem in the automation scripts, there can be major risk factors. For example, if an error is contained in the script relating to VM creation, that error is replicated (Himmel 2012:104-105). Standardisation can help lower the risk. This is achieved by creating a more consistent environment, through limiting the number of different types of VMs that are available in the cloud. Unfortunately, this does present its own risks where, due to a more constant environment, there is a greater risk for the spread of

malicious software and viruses (Himmel 2012:104-105). If one VM is breached, then VMs of the same type are also open to the same security exploit.

Governance and enterprise risk management: These elements are concerned with the establishment and execution of organisational processes, structures and controls which are used for the maintenance of information security governance, compliance and risk management (Cloud Security Alliance 2011:30). A loss of governance over the processes, structures and controls can lead to a loss of control over these issues. This provides a risk for prospective cloud users.

The loss of governance can compromise the organisation's ability to comply with regulatory and legislative procedures. The organisation's capacity to show integrity, reliability and authenticity of the information that they are storing in the cloud must be demonstrated. Cloud service providers who may not want to share usage and access logs with their users for auditability further complicate this. Unfortunately, it can be just as difficult for clients to utilise their own monitoring software for this (Convery 2010:15). These issues need to be considered by organisations. If the service provider is unable to share information, which may affect the auditability of the stored data, then the traditional data centre may be the more viable option.

Interoperability, portability and data lock-in: *Interoperability* is concerned with all the components of cloud computing having the ability to exchange with different, as well as new, components from alternate providers and continue to function. Portability refers to the ability of the applications' components to be moved and recycled in another location, despite the operating system, provider, location, infrastructure or Application Program Interface (API). However, absence of interoperability and portability can lead to data lock-in with a cloud service provider (Cloud Security Alliance 2011:64-65). This is due to a lack of standardised APIs, or procedures, which can make it expensive or very difficult for users to migrate to another service provider, as they are now "locked in" to the current cloud service provider's development environment (Convery 2010:14, 71).

Portability is an important aspect for consideration with a cloud service provider. This feature can deliver business benefits through multiple identical cloud deployments across various service providers as well as prevent *data lock-in* (Convery 2010:14; Cloud Security Alliance 2011:65). Additionally, data ownership must be established. In the event that one party no longer wishes to

do business with the other (client or cloud service provider), there must be an easy transition where the data are returned in a usable format (Antonopoulos & Gillam 2010:252). Lack of standardised APIs can mean that when a client wants to move its cloud services, they first have to migrate all their services back in-house before they can outsource it again (Convery 2010:14; Cloud Security Alliance 2011:65).

With cloud computing still maturing, standardised API and procedures are lacking. This makes it difficult for clients to transfer their data or service from one cloud service provider to another and often at great cost. This is known as data lock-in/vendor lock-in, where the cloud service provider has an interest in retaining customers by being locked into their products. This does present certain issues such as the cloud service provider ceasing to operate or raising the price of their services (Armbrust et al. 2009:15; Convery 2010:14-15). Organisations will need to ensure that their data being hosted in the cloud retain its validity, despite a service provider going out of business (Mollah et al. 2012:5).

Viability: Cloud computing is perceived as viable but there are also risks associated with *Viability*. This risk may be affected by hidden variable costs and shared reputation and accountability. In instances where companies are not acutely aware of what exactly they are being charged for in the cloud's pay-per-use model, hidden costs can render what looks to be a viable solution into a costly decision. Cloud service providers charge per hour, which may include time when a client's instances are idle (Armbrust et al. 2008:18*)*. The low costs associated with cloud computing have caused a rise in its adoption by organisations looking to outsource their data to save on IT costs. The downside of this low-cost model is the hidden variable cost risk. Organisations' scalability may be based on workload, which could fluctuate at unpredictable intervals and cause unpredictable costs due to more resources being required (Himmel 2012:109).

Shared reputation and accountability are another associated risk of cloud computing. This is due to shared resources and multi-tenant virtualisation. Various issues can arise with a shared effect. The can be explained as follows: If a cloud client causes a spam attack, which in turn causes the cloud service provider's IP address to become blacklisted, this may limit what applications could be hosted. Applications (such as spam filters) could block the provider's IP address and prevent applications from running. A further issue would be legal accountability, where the cloud service provider would not want to be accountable and would want the client, or perpetrator, to be held

accountable for their actions (Armbrust et al. 2008:18).

The *Viability* of a service provider is usually a concern for organisations. For cloud service providers, this concern is no different. If a cloud service provider goes out of business or is acquired by a competitor, this will affect the users' data and/or their accessibility (Heiser & Nicolett 2008:4). For organisations looking to utilise cloud computing for records management it may be problematic. For example, if the service provider does go out of business data could be lost or in an unusable format. Organisations cannot afford to lose their stored records, as it can cause issues related to liability and daily operations. An example of this occurred with the company *Linkup,* an online storage service. On 8 August 2008, *Linkup*, the company previously known as *MediaMax*, shut down after it lost access to an unspecified amount of client data. *Linkup* had ±20000 users. Their website reported that they were no longer offering a service. The company's CEO reported that at least 55% of the data was safe but, for the remaining 45% it was unclear how much was actually saved (Brodkin 2008).

Availability and reliability: A core benefit of cloud computing is the availability and reliability of the service (Bassett 2015:108). However, these attributes can present their own risks. An important issue is the service level commitments that are required for critical business processes. Often, the case may be that the cloud service provider may not include these offerings in their actual service. In such instances, the client must define what service level requirements the cloud service provider requires and ensure that if these are not met, there are penalties for the cloud service provider (Heiser & Nicolett 2008:3).

If a cloud service provider ceases operations and goes out of business, there is no regulated process for returning the information to its clients. Thus, contingency planning is required for these instances (Convery 2010:14). Organisations utilising cloud services may need to draw up a contingency plan. This plan needs to formulate how business operations will not be interrupted in the event of an outage. In addition, the plan should indicate how the service provider will back up existing data and/or access to critical files required to conduct daily operations (Convery 2010:64).

Discussion and recommendations

According to United States President, Barak Obama, cloud computing would "open up the government to its citizens" (Paquette 2010:247). The use of such technology would bring government closer to the social expectations of the general public. Nelson Mandela emphasised the importance of recognising the capacity for people in the 21st century to communicate as a human right. He encouraged the international community to allow the benefits of the Information Age (Paquette 2010:245). Cloud computing provides cost-effective and mutual playing field (Eccles & Armbrester 2011:14). However, security-related challenges are concerns that South African entities should be grappling with and engage with in international discussions and forums to determine adequate strategies to deal with associated risks (Carroll 2012:78). Cloud computing may further enable public entities to comply with best practices approaches, as encouraged by the World Bank, International Monetary Fund and United Nations.

Cloud computing involves computing services delivered over the internet, on demand, from a remote location, rather than a user's desktop or entity's servers (Jackson & Shelly 2012:10, 15; Laverty 2011:37-38). The computing tasks and information are available anytime, anywhere and from any device with internet access. Advantages of cloud computing are the reduction in IT-related costs, such as implementation, maintenance, hardware, application development, deployments and security (Carroll 2012:78).

Cloud computing could be used as a utility, such as electricity but, as proposed by Eccles and Armbrester (2011), the service must comply with recognised standards like those encouraged by the International Integrated Reporting Committee in August 2010. This committee was commissioned with the task of officially launching a globally accepted framework for sustainability accounting. Its tasks were to "bring together financial, environmental, social and governance information in a clear, concise, consistent and comparable format . . . The intention is to help with the development of more comprehensive information about an organisation's total performance, prospective as well as retrospective, to meet the needs of the emerging, more sustainable, global economic model" (Eccles & Armbrester 2011:13). Like South African JSE-listed private companies wanting international credibility and needing to demonstrate compliance with recognised international standards such as ISO 15489, US DoD 5015.2 and the King Commission (Institute of Directors 2009), credibility stakes should be determined for the South Africa's local government sector.

Conclusion

In striving to meet post-apartheid, democratic constitutional objectives, the South African public sector needs to participate in principles of open government, facilitate transparency, participation and collaboration (Duggan 2011). Echoing the sentiments of scholars like Allan (2009), Cox (2005, 2006), Barata, Cain and Routledge (1999), Greenwood (2012), IRMT (2012), Oyewole (2012), Shepherd (2006), Thurston (1996) and Yeo (2011), solutions need to be formulated to enable the local government sector to accurately locate and find their information sources. Public bodies need to clearly demonstrate the measures they enforce concerning the creation, management and accessibility of information sources in observance of good governance. Essential is the need to correlate the management of information sources as key components in providing proof of observance and compliance with legislative and regulatory requirements. These obligations as well as the risks associated with using cloud computing to effect good public sector records management practices should be considered by the SA local government sector in the pursuit of good governance and the attainment of clean audits from the AGSA.

References

Allan, K. (ed.) 2009. *Paper wars: Access to Information in South Africa*. Wits University Press: Johannesburg.

Antonopoulos, N. & Gillam, L. 2010. *Cloud computing principles, systems and applications*. Springer: London.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D. & Katz, R. 2009. Above the clouds: a Berkeley view of cloud computing. Available at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf. (Accessed 4 April 2016).

Asogwan, B.E. 2012. The challenge of managing electronic records in developing countries. Implications for records managers in sub Saharan Africa. *Records Management Journal* 22(3): 198-211.

Avanade. 2013. Is enterprise social collaboration living up to its promise? Available at: http://www.avanade.com/~/media/documents/resources/social-collaboration-global-study.pdf. (Accessed 20 April 2016).

Badenhorst, M. 2009. Making sense of IT governance: the implications of King III. Paper presented for CIS Corporate Governance Conference on 10 and 11 September. Available at:

http://www.icsa.co.za/documents/speakerPres/MarleneBadenhorst?BadenhorstMakingSenseOfITGovernanceTheImplicationsOfKingIII.pdf. (Accessed 15 April 2016).

Barata, K., Cain, P. & Thurston, A. 1999. *From accounting to accountability: managing accounting records as a strategic resource*. International Records Management Trust: London.

Bassett, C. 2015. Cloud computing and innovation: its viability, benefits, challenges and records management capabilities. Master's dissertation. University of South Africa, Pretoria.

Bhimani, A. 2008. Making corporate governance count: the fusion of ethics and economic rationality. *Journal of Management Governance* 12: 135-147. Available at: http://www.springerlink.com/content/k3u0303vwin14435/ (Accessed 20 April 2016).

Biggs, S. & Vidalis, S. 2009. Cloud computing: the impact on digital forensic investigations in Institute of Electrical and Electronics Engineers. International Conference for Internet Technology and Secured Transactions (ICITST): London, England.

Bouayad, A., Blilat, A., E.l Houda Mejhed, N. & Ghazi, M. 2012. Cloud computing: security challenge in Institute of Electrical and Electronics Engineers. Colloquium in Information Science and Technology (CIST), Fez, Morocco, 22-24 October.

Brodkin, J. 2008. Loss of customer data spurs closure of online storage service "The Linkup" *Network World* 11 August. Available at: http://www.networkworld.com/news/2008/081108-linkup-failure.html. (Accessed 20 April 2016).

Buckley, C. 2013. The cloud: Mitigating risks as you relinquish control. *TechRepublic* Available at: http://www.techrepublic.com/blog/tech-decision-maker/the-cloud-mitigating-risks-as-you-relinquish-control/(Accessed 20 April 2016).

Cain, P. 2002. Model requirements for the management of electronic records (MoReq): a critical evaluation. *Records Management Journal* 12(1): 14-18.

Carroll, M., Kotzé, P. & Van der Merwe, A. 2012. *Securing virtual and cloud environments in cloud computing and services science*. New York, Springer.

Carlson, T. 2001. Information security management: Understanding ISO 17799. *International Network Services* pp. 3 – 9. Available at: http://www.kwesthuba.co.za/downloads/03_ins_info_security_iso_17799_1101.pdf. (Accessed 22 April 2016).

Cervone, H.F. 2010. "An overview of virtual and cloud computing," *OCLC Systems & Services,* 26(3): 162-165. Available at:

http://dx.doi.org/10.1108/10650751011073607. (Accessed 15 April 2016).

Cloete, GS. 2007. "Governance and transparency in South Africa. *Politeia* 26(2): 192-206.

Cloud Security Alliance. 2013. About. Available at: https://cloudsecurityalliance.org/about/. (Accessed 15 April 2016).

Convery, N. 2010. Guidance for outsourcing information storage to the cloud. Available at: http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf. (Accessed 15 April 2016).

Convey, N. & Ferguson-Boucher, K. 2011. Storing Information in the Cloud. *Information and Records Management Bulletin* 161: 3-5.

Cox, R.J. 2005. *Archives and archivists in the information age*. New York: Neal-Schuman Publishers.

Cox, R.J. 2006. *Ethics, accountability and recordkeeping in a dangerous world*. London: Facet Publishing.

Cunningham, A. & Phillips, M. 2005. Accountability and accessibility: ensuring the evidence of e-governance in Australia. *ASLIB Proceedings: New Information Perspectives* 57(4): 301-317.

Dikopoulou, A. & Mithiotis, A. 2012. The contribution of records management to good governance. *TQM Journal* 24(2): 123-141. http://dx.doi.org/10.1108/17542731211215071.

Dryden, J. 2010. Standards: News, progress reports and reviews. *Journal of Archival Organisation* 8: 260-263. http://dx.doi.org/10.1007/s10502-012-9182-5.

Duggan, J.A. 2011. Silences, secrets and memory. Available at: http:archivalplatform.org/blog/secrects_silences_and_memory (Accessed 16 December 2011).

Duranti, L. & Thibodeau, K. 2006. The concept of record in interactive, experiential and dynamic environments: the view of InterPARES. *Archival Science* 6(1): 13-68. Available at: https://link.springer.com/content/pdf/10.1007%2Fs10502-006-9021-7.pdf (Accessed 4 March 2016).

Eccles, R.G. & Armbrester, K. 2011. Two disrupted ideas combined. integrated reporting in the cloud. *IESE Insight* 8(1): 13-20. Available at: http://www.forceforgood.com/userfiles/Insight%20Article%202011.pdf. (Accessed 20 March 2016).

Gartner. 2010. Gartner Global IT Council for Cloud Services Outlines Rights and Responsibilities for Cloud Computing Services. Available at: http://www.gartner.com/newsroom/id/1398913 (Accessed 22 April 2016).

Gartner. 2013. Gartner says at least 60 percent of information workers will interact with content applications via a mobile device by 2015. Available at: http://www.gartner.com/newsroom/id/2529315. (Accessed 20 March 2016).

Gellman, R. 2009. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. Available at http://www.worldprivacyforum.org/wp-content/uploads/2009/02/WPF_Cloud_Privacy_Report.pdf. (Accessed 10 April 2016).

Greenwood, P. 2012. Make information and records management a boardroom issue. *International Records Management Bulletin* 167: 28-29.

Harmon.ie. 2013. New survey reveals! Mobile 'Rogue IT' costing US organizations almost $2B. *Harmon.ie blog*, [blog] 12 September. Available at: http://harmon.ie/blog/new-survey-reveals-mobile-rogue-it-costing-us-organizations-almost-2b. (Accessed 20 April 2016).

Healy, P.M. & Palepu, K.G. 2003. The Fall of Enron. *Journal of Economic Perspectives* 17(2): 3-26.

Heiser, J. & Nicolett, M. 2008. Assessing the security risks of cloud computing. Available at: http://cloud.ctrls.in/files/assessing-the-security-risks.pdf (Accessed 22 March 2016).

Himmel, M.A. 2012. Qualitative analysis of cloud computing risks and framework for the rationalization and mitigation of cloud risks. PhD Thesis. Pace University, New York.

Hunter, G. 2004. *Developing and Maintaining Practical Archives*. New York: Neal Schuman Publishers.

Hurley, C. 2004. What, if anything, is records management? Available at: http://infotech.monash.edu/research/groups/rcrg/publications/ch-what.pdf (Accessed 5 December 2015).

ICO. n.d. The guide to data protection. Available at: http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf. (Accessed 2 April 2016).

Isa, A.M. 2009. *Records management and the accountability of governance*. PhD: University of Glasgow, Glascow. Available at: http://theses.gla.ac.uk/1421/1/2009matisaphd.pdf. (Accessed 18 March 2016).

Jackson, M. & Shelly, M. 2012. *Electronic information and the law*. Sidney: Thomson Reuters Professional Australia Limited.

JISC InfoNet. 2007. Implementing an electronic document and records management system (EDRM). Available at: http://www.jiscinfonet.ac.uk/InfoKits/edrm. (Accessed 18 March 2016).

Laverty, A. 2011. The cloud and Africa – indicators for growth of cloud computing. *The African File*, pp. 1-17. Available at: http://theafricanfile.com/ict/the-cloud-and-africa-indicators-for-growth-of-cloud-computing. (Accessed 18 April 2016).

Katuu, S. 2012. Enterprise content management (ECM) implementation in South Africa. *Records Management Journal* 22(1): 37-56.

Kenosi, L. 2011. Good governance, service delivery and records: the African tragedy. *Journal of South African Society of Archivists* 44: 19-25.

Ketelaar, E. 1992. Archives of the people, by the people, for the people. *South African Archives Journal* 34: 5-16.

Krahn, K. 2012. Looking under the hood: unravelling the content, structure and context of functional requirements for electronic recordkeeping systems. PhD Thesis. University of Manitoba, Winnipeg. Available at: http://hdl.handle.net/1993/8105/1/Konrad%20Krahn%20Thesis%20Final.pdf (Accessed 30 June 2013)

Makhura, M.M. 2001. The role of electronic records management in a service organisation. MINF Dissertation. Rand Afrikaans University, Johannesburg. Available at: http://hdl.handle.net/10210/1865 (Accessed 14 March 2016).

Mansourian, Y. 2006. Adoption of grounded theory in LIS research. *New Library World* 107 (1228/1229): 386-402.

McKemmish, S. 2001. Placing records continuum theory and practice. *Archival Science* 1(4): 333-359. Available at: http://www.springerlink.com/content/j217324514167485/ (Accessed 18 April 2016).

Mnjama, N. & Wamukoya, J. 2007. E-government and records management assessment tool for e-records readiness in government. *Electronic Library* 25(3): 274-284.

Mollah, M.B., Islam, R.K. & Islam S.S. 2012. Next generation of computing through cloud computing technology, in IEEE (Institute of Electrical and Electronics Engineers) *25th IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)*, Montreal, Canada, 29 April - 02 May.

Ngoepe, M.S. 2008. An exploration of records management trends in the South African public sector: a case study of the Department of Provincial and Local Government. MINF Dissertation. University of South Africa, Pretoria.

Ngoepe, M.S. 2012. Fostering a framework to embed the records management function into the auditing process in the South African public sector. PhD Thesis. University of South Africa, Pretoria.

Ngoepe, M. & Ngulube, P. 2014. The need for records management in the auditing process in the public sector in South Africa. *African Journal of Library, Archives and Information Science* 24(2): 135-150.

Noury, V. 2011. Cloud computing. Is Africa reaching for the clouds? *African Business* 45: 86.

Opala, O.J. 2012. An analysis of security, cost-effectiveness and it compliance factors influencing cloud adoption by IT managers. PhD Thesis. Capella University, Minneapolis.

Oyewole, O.A. 2012. "The evolution of records management in sub-Saharan Africa," *Information and Records Management Bulletin* 166: 3-4.

Paquette, S., Jaeger, P.T. & Wilson, S.C. 2010. "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly* 27: 245-253. http://dx.doi.org/10.1016/j.giq.2010.01.002

Petlane, T. & Gruzd, S. 2011. *African Solutions. Best Practices from the African Peer Review Mechanism*. Auckland Park: Jacana Media.

Queensland Government. 2013. Risks of cloud computing. Available at: http://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-risks. (Accessed 20 April 2016).

Ramgovind, S. Eloff, MM. & Smith, E. 2010. The Management of Security in Cloud Computing. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5588290 (Accessed 18 April 2016).

Rimal, B.P., Choi, E. & Lumb, I. 2010. Taxonomy, survey, and issues of cloud computing ecosystems. In: Antonopoulos, N. & L. Gillam (Eds). *Cloud Computing Principles, Systems and Applications,* Springer: London.

Rittinghouse, J.W. & Ransome, J.F. 2010. *Cloud computing implementation, management, and security*. Boca Raton: CRC Press.

Rothenberg, J. 1995. Ensuring the longevity of digital documents. *Scientific American* 272 (1): 24-29.

Samuelson, K. 2012. Can IRM save the world? *Information and Records Management Bulletin* 166: 7-11.

Shepherd, E. 2006. Why are records in the public sector organizational assets? *Records Management Journal* 16(1): 6.

Smith, K. 2007. *Planning and implementing electronic records management: a practical guide*. London: Facet Publishing.

Sprehe, J.T. 2005. The positive benefits of electronic records management in the context of enterprise content management. *Government Information Quarterly* 22: 297-303. http://doi.10.1016/j.giq2005.02.003

Sosinsky, B. 2011. *Cloud computing bible*. Indianapolis: Wiley Publishing.

Staunton, R. 2012. How to federate paper and computer-based records: turning vision into reality and saving money at the same time. *Information and Records Management Bulletin* 165: 3-6.

Stearns, J.C. 2010. Employing the Generally Accepted Recordkeeping Principles (GARP) to Identify Practices and Compliant Electronic Records and Information Management. Applied Information Management and the Graduate School of the University of Oregon. Available at: http://hdl.handle.net/1794/11208, (Accessed 10 January 2016).

Stephens, D.O. 2003. "Protecting records in the face of chaos, calamity and cataclysm. *The Information Management Journal* Jan/Feb: 33-40.

TechnologyOne. 2012. Enterprise Content Management. ECM for Local Government. Document, records and process management designers for council business. TechnologyOneCorp.com. Available at: http://www.technologyonecorp.com (Accessed 10 November 2015).

Thomas, P.Y. 2010. Cloud computing: A potential paradigm for practising the scholarship of teaching and learning. *The Electronic Library* 29(2): 214-224. http://dx.doi.org/10.1108/02640471111125177

Thurston, A. 1996. Records Management in Africa: old problems, dynamic new solutions. *Records Management Journal* 6(3): 187-200.

Wallace, M. & Webber, L. 2011. *The disaster recovery handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities and assets*. 2nd ed. New York: American Management Association.

Vaquero, L.M., Rodero-Merino, L., Caceres, J. & Lindner, M. 2009. A break in the clouds: Towards a cloud definition. *Computer Communications Review* 39: 50-55. Available at: http://www.research.ibm.com/haifa/projects/systech/reservoir/public/CloudDefinitionPaper.pdf. (Accessed 15 March 2016).

Yeo, G. 2011. Rising to the level of a record? Some thoughts on records and documents. *Records Management Journal* 21(1): 8–27.