ESARBICA JOURNAL

JOURNAL OF THE EASTERN AND SOUTHERN AFRICA REGIONAL BRANCH OF THE INTERNATIONAL COUNCIL ON ARCHIVES

Volume 36

2017

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

ACCESSIBILITY AND SECURITY OF DIGITAL RECORDS IN THE OFFICE OF THE PREMIER IN EASTERN CAPE, SOUTH AFRICA

Ndakasharwa Muchaonyerwa

University of Fort Hare, South Africa

nmuchaonyerwa@ufh.ac.za

Received: 20 May 2015
Revised: 10 October 2017
Accepted: 25 October 2017

Abstract

Digital records management systems should remain accessible and secure. Proper procedures and mechanisms should be in place to ensure security, long-term preservation and accessibility of digital records for effective e-governance. This paper investigates the accessibility and security of digital records in the Office of the Premier (OTP) in Eastern Cape. A case study was conducted in OTP for a period of 6 weeks. Questionnaires, interviews, observations and document analysis were used to collect data. It was established that the department does not place much emphasis on the security of digital records since there are no existing facilities regarding the storage of digital records. The department does not have a specific policy regarding the accessibility and management of digital records. There were concerns about manipulating records in digital recordkeeping systems which generated uncertainty about the use and security of digital systems. It was concluded that with the increasing use of information and communication technologies (ICT) in OTP, and in preparation for the switch to e- government there is a need for a dedicated section/unit with the responsibility for the security and management of digital records. The need for expertise in managing digital records has been identified as a critical success factor for implementing a document records management (DRM) programme. Staff should be encouraged to get training so as to be knowledgeable in the use of the technologies that generate digital records.

Keywords: Records Management, Accessibility, Security, Provincial Governments, South Africa

Introduction

In the context of this study accessibility is the ability to provide information and communication technologies (ICTs) tools that provide services and information to people. The adoption of ICTs in service delivery, which is in line with e-government strategies, has resulted in the creation and use of digital records in many governments. In South Africa, this strategy is believed to increase the efficiency of the processes such as those supporting financial and human resources management. Records in digital form consist of one or more objects such as a web page, e-mail, file or document (Smith 2007). The purpose of digital records is to increase accessibility and utilization of records between the public and the government. Records which are created using electronic/document records management systems (EDRMS) should remain available, usable, understandable and authentic over a long period of time. DRM literature indicates that digital records and data can be easily deleted and are subject to unauthorized alterations (Stair and Reynolds 2006). The survival and the readability of records can easily be endangered in the electronic environment. Thus, the need to design and build systems that ensure the survival of digital records is important (Shepherd 2006).

There are also challenges to security which may lead to record loss such as data corruption in which the integrity, reliability and confidentiality of digital records can be compromised. Security refers to the policies, procedures, and technical measures used to prevent unauthorized access, alteration, theft and physical damage (Laudon and Laudon 2005). There are a number of security dilemmas in digital records management. Some of the dilemmas include unauthorized access of patients' records, organization financial records and employees 'records. The security of such records is essential to ensuring their reliability, integrity and evidential value. Those who are responsible must understand the sensitivity of the records they hold (Freda 2014). Government departments need to control access to their records which contain personal and operational information that should be protected against unauthorized access. The efficient and effective delivery of services is reliant on timely access to records. It is therefore important that government departments balance security requirements against the need for easy and appropriate access to records for business and legislative purposes. Achieving this balance should be the result of a process which defines documents security and access requirements across the entire government departments. Fang-Ming, Tser-Yieth, Chiu-Tsu, Chun-Min, and Chu-Mei 2015) observed that appropriate disclosure of records regarding personal information can effectively increase confidence, trust and satisfaction of participants. Information transparency and accessibility significantly affect the brand image of the organization.

However, the management of records in electronic format is not fully taken seriously in most government departments because some of the staff who works with such kind of records are not fully equipped or have skills on how to properly take care of digital records. It is a responsibility of the government to make sure that every individual who works with e-records is fully trained on how to manage the e-records so that each time they are needed they can be easily accessible and available (Kamoun and Almourad 2014). Nevertheless, despite the crucial role played by records management, there is consensus amongst some researchers that many organizations including the government departments pay little attention to the management of e-records (Chinyemba and Ngulube 2005; Kamoun and Almourad, 2014). In some cases, departments handle recorded information carelessly without realizing that e-records constitute a major resource compared to finance, money and other devices (Ngulube 2006). The anxiety by governments to adopt electronic or digital records management systems (EDRMS) does, however face limitations especially in the developing world. In most cases, both government officials and the public who may want to use government services maintained in digital form lack basic skills in accessing the information. This obviously impacts the relationship between the government and the users of its services. Ngulube (2007) avers that government information especially in the Sub-Saharan Africa (SSA) is not properly organized as records management systems in many countries lack the necessary equipment, infrastructure and trained records managers hence they are collapsing. According to Ngulube (2006) the transformation from paper based records to digital records is happening at a time when many records managers in SSA do not have the necessary skills to deal with digital records in terms of security and accessibility.

The Office of the Premier (OTP) provides guidance and focus for the province through the development and implementation of policies, and the monitoring and evaluation of the performance of departments to ensure service delivery to all the people in the province. The

Promotion of Access to Information Act which, came into effect in 2001, places the obligation on government to make information accessible to the public in order for them to realize their constitutional right of access to information. Citizens of South Africa want better quality services from all levels of government for example they want respectful and courteous service, shorter queues and no misplacement of documents. The *Batho Pele motto* on transforming public service delivery seeks to introduce a citizen oriented approach that put people first. To this end the Office of the Premier monitors the level and quality of government services and promotes a culture of access, openness and transparency that in turn should build more confidence between government and the public it serves (South Africa 1997). To this end the organizational structure of OTP was amended to ensure that it fulfils its mandate and is better aligned to national imperatives that address local challenges. The purpose of the study is to examine the accessibility and security of digital records in the Office of the Premier in Eastern Cape Province. The knowledge generated from this study may be helpful in providing direction in terms of factors needed in the improvement of digital records. The study will serve as a catalyst in the modification and information of digital records management strategies and policies in the South African government. The findings will help provide the government with quick and accurate data for effective policy formulation to ensure easy access to records by authorized people.

Accessibility and security of digital records in government departments

Significant amount of government records are created, received, stored and sent in electronic form. These records include email messages and their attachments, word processing or spreadsheet documents, web pages and databases. Also formal documents such as tax returns, license and permit applications and other documents lodged with agencies, generally originate in electronic format. Much of this electronic information will only ever exist in digital form. Literature show that in Africa, many countries are lagging behind in the area of digital records management because of the lack of e-records management policies and inadequate expertise (Laudon and Laudon 2005; Kemoni 2009). There are also challenges to security, which may lead to record loss such as data corruption and unauthorized access in which the integrity, reliability and confidentiality of digital records could be compromised (Laudon and Laudon 2005).

Goodwin, Susar, Nietzio, Snaprud and Jensen (2011) study on the accessibility analysis of e-government websites from the United Nations member states revealed that, with few exceptions, the governments' web sites of developed countries are more accessible than those of developing countries. The study also found that e-government web sites that are recognized as mature and of high quality are more likely to be accessible. In Africa, Kuzma (2010) assessed the accessibility of e-government web sites belonging to 12 developing and developed countries. Serious accessibility issues for the tested e-government sites, even for websites belonging to governments who claimed to adherence with the accessibility standards and United Nations legislations were identified. The web sites were not secure to unauthorised access and they were not user friendly to all categories of users especially those with disabilities.

A number of security dilemmas in digital records management are witnessed. For example, thousands of patients' records were accessed online on a government internet server, where records of state hospital patients from around the Eastern Cape are stored (*Daily Dispatch* 2010). Again, the revelation about WikiLeaks and its release of 250, 000 confidential state department cables is a challenge faced by both public and private sectors in the provision of security and access to e-records (Verace 2010). In the era of WikiLeaks, it is clear that lack of security and unauthorized access to digital records management systems (DRMS) in the public sectors presents a significant global risk particularly in the industry that gets a lot of attention for example, the financial services, government and health.

Sanders (2009) further argues that the security risks are also related to changing regulations such as poor or inconsistently communicated policies. Governments around the world have come up with policies and principles, which require the management of digital records. In South Africa, all records created and received by government bodies shall be managed in accordance with the records management principles contained in section 13 of the National Archives and Records Service Act (no. 43 of 1996 as amended). In accordance with the section 13 of the National Archives and Records Service of South Africa (NARS) Act (no. 43 of 1996), the National Archivist, among other things, determines the conditions subject to which electronic systems should be managed to ensure that sound records management practices are applied to electronic records systems from the design phase onwards. The Promotion of Access to Information Act (no. 2 of 2000) (PAIA) by the South African government outlines the need for proper records management. The Act gives effect to the right provided in the Constitution of access to any information held by the state and any information that is held by another person that is required for the exercising or protection of any rights.

The earlier studies revealed that many digital records management systems (DRMS) have been developed with accessibility barriers due to either lack of awareness of the importance of web accessibility or the lack of resources and capabilities to design user friendly accessible DRMS. Regardless of the reasons behind these accessibility barriers, previous studies emphasized the need for e-government DRMS to be accessible in order to provide people with an opportunity to access the e-records and valuable services (Kamoun, Mohamed and Almourad 2014).

Problem statement

Empirical studies around the world (Goodwin et al., 2011; Isa, Suhami, Safie and Semsudin 2011; Kuzma 2010; Abdul Latif and Masrek 2010) revealed that many governments are struggling with issues of handling e-records due to either lack of resources and capabilities to design accessible and secured web sites. Wamukoya and Mutula (2005) reported major drawbacks in the security measures and confidentiality of e-records in public sectors in the eastern and southern African countries. Government departments that have computerized seem to have a framework for handling digital records. A number of security dilemmas in e-records management have been reported. Thousands of patients' records were accessed online on a government internet server, where records of state hospital patients from around the Eastern Cape are stored (*Daily Dispatch* 2010). Government departments need to control access to their records which contain personal and operational information that should be protected against unauthorized access. It is clear that poor digital records management practices in public sectors presents a significant global risk particularly in the industry that gets a lot of attention for example, the financial services, government and health. Kamatula (2010) reported that digital records, just like paper records, have to be retained for a long period to serve as evidence of organizations' transactions. Proper procedures and mechanisms should be in place to ensure security, long-term preservation and accessibility of digital records for effective e-governance. The findings will serve as a guide on the management of digital records and ensure that those responsible and work with e-records receive training.

Research Questions

1. Does OTP have security and preservation measures in place for the management of digital records?
2. Does the department comply with the legal l framework that governs the security and accessibility of digital records in governmental bodies?
3. Does the Office the Premier have a policy on records management?
4. What are the challenges of accessing digital records in OTP?

Methodology

A case study was conducted in OTP for a period of six weeks. The study adopted a mixed method approach by using quantitative and qualitative methods to examine the accessibility and security of digital records in the Office of the Premier. The rationale for using both methods is that neither a quantitative nor qualitative method alone would have been sufficient enough to capture DRM in OTP. The investigation focused on the relevant sections (directorates) and intentionally selected personnel in the department for interviewing. A sample of 40 was selected from the target population of 487 staff members using the internal directory of OTP and also with the help of the records manager. Only those who were involved in the creation and management of records were selected. The participants in the study involved seven registry staff members, three library staff members, the records manager, the Information Technology manager, four ICT support staff, the legal service manager, the Director General of the administration and support services, the Chief Information Officer, the security manager, two senior managers and five assistant managers from Human Resources Management (HRM), two managers from the communications directorate and one supervisor from the supply chain and ten HRM practitioners. A computer software, SPSS was used to analyse quantitative data which was then presented using tables, pie charts and graphs. Qualitative data was presented by thematic categorization of themes based on objectives. Out of 40 respondents that were targeted only 30 responded to the questionnaire. Gender of respondents comprised of seventeen (57%) male and thirteen (43%) female. Responses consisted of 17 top management staff and 13 other staff members from different directorates.

5. Profile of Respondents

The majority (56.7%) held positions of a director general (DG), managers, assistant managers and supervisors, five (16.7%) were administration assistants from the HRM and communications directorates, two (6.7%) were holding positions of senior managers and above whereas one held the position of a records manager. The results are in indicated in Figure 1.

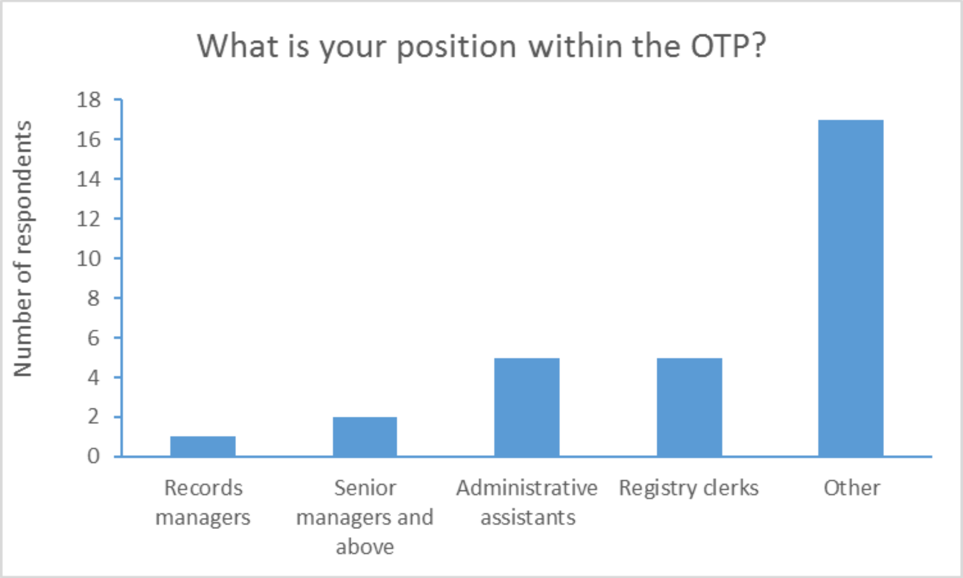

Figure 1: Position occupied (n=30)

Findings and discussions

Security and preservation measures in place for the management of e-records

Kamatula (2010) reported that digital records, just like paper records, have to be retained for long periods to serve as evidence of organizations' transactions. Proper procedures and mechanisms should be in place to ensure security, long-term preservation and accessibility of e- records for effective e-governance. The respondents were asked if OTP had a system in place to ensure security and protection of digital records. The majority (60.0%) had no idea, ten (33.3%) said there was a system in place to ensure protection of digital records in OTP whilst two (6.7%) did not respond. The results are indicated in Table 1.

Table 1: System in place to ensure access and security (n=30)

	Frequency	Percentage
No idea	18	60.0
Yes	10	33.3
No response	2	6.7
Total	30	100

The variations in these responses were attributed to lack of awareness of digital records management systems. Interviews with the records manager indicated that the department does not place much emphasis on the security of its records but tries to secure confidential records, which are stored in the EDRMS. The records manager reported that there was an offsite server where the information is stored should the system crash. Personal observations revealed that there were no guidelines regarding the security of digital records. It was reported that they are no existing storage facilities for digital records except the database in the proposed EDRMS solution being implemented. Most of the records exist in paper based format. Interviews were also conducted with the Chief Information Officer (CIO) and the records manager on how records generated in the department are accessed and protected. They shared the following sentiments:

> *In terms of access no staff member should provide information and records that are not in the public domain to the public without consulting the Chief Information Officer. The department does not have specific security policy regarding the security and access of its digital record".*

.

> *All staff members were to follow specific guidelines regarding requests for information as stipulated in the Promotion of Access to Information Act (no.2 of 2000).*

However, all the interviewees were concerned that the level of secrecy is still a problem in the Office of the Premier. For example, breaches of security were a factor blocking trust in the use of digital records.There were concerns for protection and security measures in place to ensure the confidentiality of digital records in the department. The CIO was of the view thatprotecting the security and confidentiality of digital records stored on databases was a problem since it can be easily corrupted. There was concern about manipulating records in digital recordkeeping systems which generated uncertainty about the use of digital systems as records could be easily deleted.

In terms of access to digital records, the Information Technology (IT) security manager said that:

> *Access to server rooms is managed with a key card access. Not all staff can access confidential records.*

The senior managers from HRM further mentioned that not all users could access confidential records in digital form. For example, there are people who can view the documents while others can access depending on the level of access security one has. Access to storage areas where electronic records are stored is limited to the IT staff that had specific duties regarding the maintenance of the hardware, software and media. The research done by Mutiti (2001) revealed that, in most cases the responsibility of managing digital records is left to IT specialists because records managers are not fully conversant with their roles in digital records management programs. The records manager reported that currently the department is compiling a disaster recovery plan which talks to the retrieval of information should the system crash. Tshotlo and Mnjama (2010) stated that a disaster preparedness plan is an important tool central to the protection and preservation of e-records, and it should be incorporated into the overall management plans of the organization.

The researcher also wanted to know how the department deals with threats of: viruses, unauthorized access to digital records, environmental security and database security. Interviews with the IT manager indicated that he was responsible for the day-today maintenance of electronic systems that store digital records. The IT manager reported that he ensures the systems that manage and store records are virus free. All users (employees) of records within OTP are provided with usernames and passwords to access e-records. Lack of ICT skills for OTP employees including the records personnel was highlighted as a major problem in promoting the use of digital records inthe department. The IT manager also reported that personnel with ICT training, including managers with experience in evaluating and implementing EDRMS solutions were needed for the viability of DRM to be realized in the department. He further mentioned that although the environment is securely protected, there is lack of skills to contribute to the policies and regulations that govern the way e-records are created, used and managed. The IT manager said that there is lack of equipment that ensures e-records remained accessible. Kamatula (2010) reported that proper procedures and mechanisms should be in place to ensure long-term preservation and accessibility of e-records for effective e-governance.

Legal framework that governs the security and accessibility of digital

Interviews were conducted with the Legal Services Manager on whether the department complies with the legal and regulatory framework for digital records management. He mentioned that:

> *All those who work with electronic records must comply with the South African National Archives and Records service Act (NARS). The Act requires all the government departments to develop a policy that talks to the management of electronic records as stipulated in section 5 of the NARS Act.*

The South African National Archives and Records Service Act specifies requirements for creating authentic digital records that are usable and reliable for as long as they are required for functional, legal and historical purposes. The South African National Archives and Records Act as amended authorizes the use of digital systems to manage public records. The Act requires public agencies to use Electronic Document and Records Management System (EDRMS) to create and manage their records. Therefore, the department is aware of the legal requirements. Government departments are required to develop a records management policy that regulates records management activities. For the policy to be effective, it has to be endorsed by the head of department as well as the senior management. It should be communicated and implemented throughout the organization. The respondents were asked if OTP had a records management policy. The majority (90.0%) reported that OTP had a records management policy whilst three (10.0%) did not know whether the department had the records management policy. The respondents were further asked if the policy is endorsed by the Director General. The majority of the respondents (86.7%) indicated that the policy was endorsed by the director general and communicated to all staff members whereas four (13.3%) were not sure if the policy was endorsed by the Director General. The researcher wanted to know if the RM policy covers the security and access of digital records. However, respondents were not sure if the policy covers digital records accessibility. In order to get clarity on whether the policy covers the security and accessibility of digital records, interviews were held with the records manager who reported that the department is currently implementing the digital records management system and the policy is still work in progress. As a result, there is currently no separate policy for digital records management in the department. The findings agreed with Ngoepe (2008) who found that out of 30 organizations surveyed in South Africa 25 did not have a digital records management policy. The absence of a digital records management policy in the department may suggest that digital records were not secured, accessed and managed in a systematic manner.

Challenges of accessing digital records in the OTP

Majority of the respondents (66.7%) indicated that shortage of DRM skills was the biggest challenge, followed by inadequate expertise reported by (50%), ICT facilities (46.7%) and inadequate legal and regulatory system indicated by (26.7%). It was also reported that resistance to change was the most notable factor facing OTP department. It was revealed by the records manager that most employees were not comfortable with the EDRMS solution being implemented in the department because they fear losing their jobs. Those who were interviewed highlighted that there was no integrated approach to managing digital or electronic records in the Office of the Premier. The implementation of the EDRMS solution was received with less enthusiasm by the staff. It is probable that its introduction was not supported but the necessary change management training that would have helped in dispelling the fear that the new solution would lead to loss of jobs. Due to these challenges, OTP is faced with various challenges relating to members accountable for documents. These factors negatively impact on the level of service delivery offered by OTP staff. In the same vein, Mutiti (2001) found that there was a lack of standards, practices and procedures for e-records management; inability to provide guidance on e-records created in government agencies being mismanaged and overlooked and in most cases records often gets lost.

Conclusion

Staff expressed great concern about the security of e- records. They argued that information recorded electronically is not secure and that confidentiality is easily breached when records are kept in digital systems. There was no compliance with policies and procedures that guide the security of digital records in OTP. Those who were managing the e-records did not receive training on how to manage records in electronic format.

Recommendations

- There is urgent need to tighten the current security and preservation practices of digital records in OTP. Agencies must ensure that official records are protected from unauthorized or unlawful access, and that measures are in place to prevent loss, damage and destruction. This must be balanced with the need for official records to be readily accessible to authorized persons.

- There should be distinction between the physical and content security and preservation of digital records. The office of the Chief Information Officer should spearhead the formulation and implementation of a policy as well as rules and regulations to govern the security and preservation of digital records. The policy must be in line with similar policies as practiced under the National Archives and Records Service Act (no. 43 of 1996 as amended).

- The need for expertise in managing digital records has been identified as a critical success factor for implementing a DRM programme. It is recommended that OTP department develops and encourages its staff members to get training so as to be knowledgeable in the use of the technologies that generate digital records. A detailed training plan needs to be developed around the training needs of the department. OTP must ensure that financial resources are available to support the training needs as well as facilities that could enhance digital records management programme.

Areas of further research

Further research should be conducted on the capacity building strategies to manage digital records in government departments. More research is also required to establish the impact of the current state of digital records management on the proposed Promotion of Access to Information Act (PAIA) legislation initiatives in government.

Acknowledgements

The university of Fort Hare through the Govan Mbeki Research and Development Centre (GMRDC) funded the work. This work is part of the author's postgraduate studies.

References

Abdul Latif, M. and Masrek, M. .N. 2010. Accessibility evaluation on Malaysian e-government website. *Journal of E-government Studies and Best Practices* 2010: 1-11.

Chinyemba, A and Ngulube, P. 2005. Managing records at higher education institutions: a case study of the University KwaZulu-Natal, Pietermaritzburg Campus. [Online]. Available WWW: http://general.rau.ac.za/infosci/raujournal/default.asp?to=peervol7nr1 (Accessed 10 November 2010).

Daily Dispatch. 2010. East London: Daily Dispatch Publishers.

Goodwin, M., Susar, D., Nietzio, A., Snaprud, M and Jensen, C. S. 2011. Global web accessibility analysis of national government portals and ministry web sites. *Journal of Information Technology and Politics* 8(1):41-67.

Fang-Ming, HSU, Tser-Yieth, C., Chiu-Tsu, F., Chun-Min, L and Chu-Mei, C. 2015. Factors affecting the satisfaction of an online community for archive management in Taiwan Program. *Electronic Library and Information System*s 49(1): 46-62.

Freda, A. 2014. Assessment of records management practices among the administrative staff of university of education, Winneba – Kumasi (UEW-k) and Mampong (UEW-M) campus. [Online]. Available WWW: http://ir.knust.edu.gh/bitstream/123456789/7540/1/Adu%20Freda.pdf (Accessed 16 September 2017.

Isa, W., Suhami, M., Safie, N and Semsudin, S. 2011. Assessing the usability and accessibility of Malayisa E-government website. *American Journal of Economics and Business Administration* 3(1): 40-46.

Kamatula, G.A. 2010. E-government and e-records challenges prospects for African records managers and archivists *ESARBICA Journal* 29:160-181.

Kamoun, F. and Armoured, M. B. 2014. Accessibility as an integral factor in e-government web site evaluation: the case of Dubai e-government. *Journal of Information Technology and People* 27(2): 208-228.

Kemoni, H. N. and Wamukoya, J. 2000. Preparing for the management of electronic records at Moi University, Kenya. *African Journal of library Archives and Information Science* 10(2):125-138.

Kuzma, J. 2010. Global E-government web accessibility: a case study. *Proceeding, British Academy of Management 2010 Conference,* University of Sheffield, Sheffield, September 14-16.

Laudon, K. C. and Laudon, J. P. 2005. *Essentials of management information systems: managing the digital firm*. 6th ed. New Jersey: Pearson Education.

Mutiti, N. 2001. The challenges of managing electronic records in the ESARBICA Region. *ESARBICA Journal* 21(1):57-61.

Ngoepe, M. (2008). Strategies for preservation of electronic records in South Africa: implications on access to information. Paper read at Poussiere d'toiles' 2nd annual knowledge, archives and records management (KARM) conference in Polokwane. SA,6-7 May 2008.

Ngulube, P. 2007. The nature and accessibility of e-government in Sub Saharan Africa. *International Review for information Ethics* [Online]. Available WWW: http://www.i-r-i-e.net/about irie.htm (Accessed 7 November 2017).

Ngulube, P. 2006. Nature and accessibility of public archives in custody of selected archival institutions in Africa. *ESARBICA Journal* 25:106-124.

Sanders, L. 2009. Electronic document management: seven fundamentals that should never be compromised. [Online]. Available WWW: http:// www.webcache.googleusercontent.com/search (Accessed 13 September 2017).

Shepherd, E. 2006. Why are in the public sector organizational asserts? *Records Management Journal* 16(1):6-12.

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

South Africa. 2000. *The Promotion of Access to Information Act* (Act no. 2 of 2000).

South Africa. 1997. White paper on transforming service delivery. [Online]. Available WWW: http://www.info.gov.za/whitepapers/1197/18340.pdf (Accessed 12 December 2012).

South Africa. 1996. *National Archives and Records Service Act* (Act no. 43 of 1996).

Stair, R. M. and Reynolds, G. W. 2006. *Principles of information systems: a meaningful approach*. Bonston: Thomson Course Technology.

Tshotlo, K. and Mnjama, N. 2010. Records management audit: the case of GaboroneCityCouncil. *ESARBICA Journal 2 9* :5-35.

Verace, M. 2010. Information risk in the whikleaks era. *Article*. [Online]. Available WWW: http://www.cio.com/aticle /print/645710 . Accessed on 17 December 2013.

Wamukoya, J. and Mutula, S. M. 2005. Capacity building requirements for e-records management: the case in East and Southern Africa. *Records Management Journal* 15(2):71-79.