INFORMATION TECHNOLOGY: A CHALLENGE TO THE CREATION AND PRESERVATION OF TRUSTWORTHY ELECTRONIC RECORDS IN THE PUBLIC SERVICE OF NAMIBIA

Cathrine T Nengomasha
University of Namibia, Department of Information and Communication Studies
Email: cnengomasha@unam.na

Patrick Ngulube
University of South Africa, Department of Information Science
Email: ngulup@unisa.ac.za

Received: 29 March 2009
Revised: 5 July 2009
Accepted: 1 May 2010

Abstract

As organisations increasingly adopt the use of information and communication technologies, the corresponding increase in the creation of electronic records has brought about a number of records management challenges. These manifest themselves in a number of ways. Problems associated with the management of electronic records are organisational and technical. This article focuses on the technical problems, which are normally looked upon as the "usual" IT problems but have a significant impact on the creation and preservation of trustworthy electronic records. Using examples from the public service of Namibia, the article reiterates the call for collaboration between records managers and information technology (IT) professionals in designing systems that take cognisance of records management requirements, and concludes by calling upon records management professionals to make IT professionals understand what records management principles are and how they may contribute to the creation and preservation of trustworthy electronic records.

Keywords: Electronic Records, Trustworthy Records, Information Technology, Records Management

Introduction

Information and communication technologies (ICTs) are increasingly being used in organisations, which has resulted in an increase in the generation of electronic records. Records are a vital resource of all organisations, whose value for providing evidence and supporting accountability and transparency relies on their authenticity, integrity, accessibility and trustworthiness as well as preservation over time. Duff (2001) points out that the "the trustworthiness and integrity of records in electronic form is often questioned and their long-term preservation creates many challenges". In an electronic environment, technological problems which are looked upon as the "usual" IT problems and include fragile media, virus attacks, poor back-up practices, inadequate resources such tapes for back-ups, absence of systems documentation, lack of data formats and metadata standards, hardware and software obsolescence, inadequate bandwidth, inadequate data storage capacity, and inadequate security, have serious implications for the creation of trustworthy records.

Technical problems and trustworthy records

Several definitions of records, such as those of the International Standard on Records Management (ISO 15489-1:2001(E)) (International Organisation for Standards 2001) and the International Council on Archives (Erlandsson 1996), agree on one thing and that is, records are a result of an activity, be it a business or a personal transaction. Records provide evidence and for them to be able to do this they need to be trustworthy.

Characteristics of a trustworthy record include reliability, authenticity, usability, and integrity. Reliability refers to records whose content can be trusted as a full and accurate representation of the transactions which they attest to. Authentic records are what they purport to be and authenticity guarantees that the record is not changed or manipulated after it has been created or received or migrated over the whole continuum of records creation, maintenance and preservation (Duranti, as cited in Sannet and Park 1999). Integrity refers to the complete and unaltered characteristic of a record. Usability refers to a record's

ability to be located, retrieved, presented and interpreted (Amadeus n. d).

Several writers (Asproth 2005; Duff 2001; Gibbs and Heazlewood 1999) have written about the technical problems which include hardware, software, data formats, storage capacity, fragile media and security. Goldstein (as cited in Asproth 2005: 28) states that “the major threat to archived material today is not the fire hazard but the rapid development of different file formats for documents…”. Many software systems do not handle different versions of data, which has become a major archival problem. Dollar (as cited in Asproth 2005) gives the example of geographic information systems which update maps electronically without saving previous versions. Gibbs and Heazlewood (1999) explain the problem of changing data formats which is linked to the problem of rapidly changing data formats. The consequence of this is that electronic records will become unreadable in the long run. Wilson (as cited in Asproth 2005) discusses the problems of storage capacity, low media durability and poor security for electronic files.

Duff (2001) summarized some of the problems posed by electronic records as follows:

- Records are system-dependent, and the hardware and software they depend upon is continuously upgraded. Therefore, records require constant migration to ensure their long-term preservation and access. Migration, however, is often problematic because of lost or missing documentation or poor record-keeping procedures;
- The authenticity of electronic records is often questioned because of possible changes to the content or structure of the records over time or across some migrations. Each migration poses the risk of altering part of the record and thereby affecting its authenticity;
- The decentralising of systems has shifted the responsibility of managing records from records professionals to end-users. Unfortunately, users lack knowledge about what to keep, or how to describe, file or maintain records. Therefore the evidence needed to retrace one's steps or to discover what happened is often difficult to locate;

- Organizations establish tight controls over their paper systems but fail to regulate their electronic systems in a similar manner. The lack of control over email systems is leading to concerns over litigation; and
- Links between paper and related electronic records are lacking and few actions are captured completely in either the paper or electronic system; and records provide evidence of actions but systems often fail to capture the necessary information about the context of the creation and use of the records.

Scope of the study and the research problem

Central to the study were the problems associated with electronic records in the public service in Namibia. One such problem investigated was the shift of control over the creation and management of information from centralised records keeping systems to the individuals through the use of information and communication technologies (ICTs).

The study was based on the assumption that the Government of Namibia has embarked on e-government, which should result in an increase of electronic records and a corresponding increase in Government's reliance on electronic information. It focussed on e-records readiness and the creation and preservation of trustworthy electronic records. E-records readiness was investigated in order to establish the status of records management in the public service of Namibia and to assess whether or not the environment *was* conducive for the creation and management of electronic records. The investigation of records trustworthiness was pertinent to the study to ensure that records provide evidence in support of transparency and accountability.

The main question to be answered by the study was, "How can the electronic records environment in Namibia's public service be strengthened to support e-government?" This was answered through a number of sub-research questions which included:

- Is Namibia e-records ready to support e-government?

- To what an extent have records keeping requirements been incorporated in electronic information management systems in the public service of Namibia?
- How can electronic records management in the public service of Namibia be strengthened to support accountability, and transparency?

Research methodology

The study, a multi-case study of eleven public service institutions, employed a qualitative approach using interviews, document search, and observation data collection methods. The eleven cases comprised seven government ministries, two local authorities and two regional councils. Eighty-five people were interviewed, including action officers, IT staff, records keeping staff, heads of records function, and National Archives of Namibia staff. The selection of the institutions was initially meant to be purposefully done. The selection of the respondents in the Ministries was also through convenience sampling. The selection of the two respondents from the National Archives, mandated with the task of providing a records management service to the public service; and the two from the Office of the Prime Minister, spearheading the e-government initiatives, was task and responsibility driven. Data was analyzed using content analysis and presented in the form of narrative interpretations, illustrative quotes and tables.

Responsibility for strategic development of IT resources and systems
The researchers asked the question: “Who is responsible for the strategic development of IT resources and systems?” Six Ministries out of the seven replied that they had a Ministerial IT Committee. The IT officer in Ministry B explained, “There are two levels. The Office of the Prime Minister outlines the whole IT strategy for Government. In the Ministry, the Ministerial Information Technology Committee is responsible for all IT related issues with the guidance of the Information Technology Division of the Ministry”. When asked if records management is represented in the Committee, the response was, “The Director of General Services is the Chairperson and represents records management”. In Regional Councils the Chief Control Officer

who is directly responsible for the records management function is also in charge of IT. In Ministry A, the Director Human Resources and Finance is in charge of the records management function as well as the IT Division. In Local Authority B the head of IT Division is in charge of the records management function and supervises the registry.

Although most institutions studied had a member who was meant to represent the records management function on IT Committees, these representatives were not knowledgeable about records management so their input on records management issues was very minimal. Electronic information systems design that excludes records management professionals disregards the requirement, according to the records continuum theory, that even at the design stage of these systems records management issues should be taken into consideration.

Electronic information systems

Several electronic information management systems could be found in the institutions studied. Electronic information systems include those designed and maintained by the Office of the Prime Minister, Department of Public Service Information Technology Management, those designed and maintained by external consultants – local and foreign, and back-office systems created by the officers. Most systems were developed by consultants and in most cases, the IT officers in various Departments were not in a position to give details on these systems.

Ten of the eleven institutions had systems developed and maintained by foreign companies. These were based in South Africa, Australia, Finland, Sweden, Mauritius and Namibia. One officer commented that some of the local companies are just fronts for foreign based companies. He referred to a case where they wanted to migrate from a system supposedly developed and managed by a local company. The company had no system documentation and had to consult its partners in a foreign country.

The study established a number of in-house (department or individual) developed systems which were completely controlled by the individuals concerned. Problems with individual software as identified by Meijer (2001) were also identified in the public service of Namibia.

One such problem was a lack of control of these systems. Most of them did not have any system documentation, with changes made to the system being in "people's heads" as one respondent put it. Individual software was not entirely maintained on the main server. As one respondent put it "all documents of staff are not backed up on the server …" and in another Ministry, "We have a lack of back-up with our in-house system. Even IT [Division] was not prepared for a long time to allow us to save on the server. Sometimes when one of our [Departmental] servers crashed we lost our mapping capability. We used to run tapes but with the computers we are using, we cannot access information on our earlier data". This study confirms problems caused by hardware and software obsolescence, and changes in data formats referred to by Dollar (as cited in Asproth 2005); as well as Meijer's (2001) findings regarding the problems of individual software which he spelt out as follows:

- Introduction of office software applications confronts organisations with lack of control over the creation and capturing of data. It may be difficult to find out for example, the final version of a document.
- Frequent release of new versions of office software applications may also present a serious problem. Lack of compatibility between software versions could hamper long-term access to data (Meijer 2001: 262).

Some threats that records of evidence in the public service of Namibia faced were that records were either created or captured in a fragmented way. Some records were not captured at all and there were no mechanisms to ensure that this was done. Secondly, those few records that were captured might not be accessible because of software incompatibility. Reported here is a situation similar to one described by Lipchack and McDonald (2003) of electronic records being created in a complex environment of fragmented and incompatible information systems.

E-mail systems

All government ministries, regional councils and local authorities had e-mail systems. There were mixed reactions towards e-mail use. In one ministry a Deputy Director said, "It is policy in this ministry that every officer should have access to e-mail". An Acting Chief Executive Officer in one of the local authorities did not share the same sentiments. "I am careful to install e-mail for each and everyone.

Viruses and misuse of e-mail are a problem. In our offices only two officials are committed to e-mail".

E-mail use had several problems that were highlighted by the respondents. These included limited storage capacity and bandwidth of the system. Some were constantly reminded to delete e-mail messages by the systems administrators and in some cases this was done automatically by the systems administrator to create space. The problem was that destruction was done with no set guidelines on what should be destroyed or not and what should be done with the ones to be preserved. As one Deputy Director commented, "There are no guidelines on electronic records. I delete the largest files first".

To get round the problem of limited storage capacity, some officers indicated that they used non-official email addresses to receive official documents. Another reason for using non-official email addresses was inadequate bandwidth problems. Officers explained that they preferred to use non official email addresses such as Yahoo as the government email system was unreliable, down constantly and extremely slow to open documents. This resulted in official documents not being kept in official government systems and having to rely heavily on individuals to ensure that the documents are brought back to the institution for filing. In an environment where there was a poor culture of filing documents in the central registries, the chances of these e-mail documents coming back to be filed were quite remote as this culture may have been transferred to the electronic environment. This study confirmed one of Meijer's findings that "Control over e-mail tends to be highly individual and often lacking in organisational control; and loss of control is an important problem for the management, retrieval, and use of messages…" (Meijer 2001: 261).

The study confirmed findings of a study by Keakopa (2007) carried out in the Namibian public service which revealed the use of e-mail technology in the Public Service of Namibia with no clear guidelines on how to deal with the management of e-mail records. Studies in Botswana by Keakopa (2007) and Moloi (2007) and in Lesotho by Sejane (2005) on electronic records management in the public sector came up with similar findings. Keakopa (2007) stated that the public service of Namibia's IT policy addressed e-mail communication but was not effective as most civil servants seemed to be unaware of the

policy. This study confirmed this observation but also discovered that the policy does not spell out the need to effectively manage e-mail records. Although e-mail usage had grown in the public service of Namibia, it had not entirely replaced “paper communication”.

Electronic records management systems (ERMS)
The study established that there are no electronic records management systems running in the public service of Namibia. Electronic records management systems are distinguished from electronic information systems within organisations by the role they play in providing organisations with evidence of business transactions. Non-record information systems, on the other hand, store information in discrete chunks that can be recombined and reused without reference to their documentary context.

A system was acquired by the Office of the Prime Minister to be applied to the entire public service. During interviews the Office of the Prime Minister indicated that the records keeping requirements which the system must satisfy were drawn up using the DoD 5015-2 (Department of Defence 2002). However, the National Archives of Namibia which is in charge of records management in the public service of Namibia indicated lack of awareness of the records keeping requirements that the system met, and in one of its reports it stated that “Government approved the purchase of an ERMS without consultation of the draft specifications which the National Archives had drafted (National Archives of Namibia 2007). This signifies a lack of coordination between the two government institutions. Although the Office of the Prime Minister is in charge of e-government, the management of electronic records is the mandate of the National Archives.

Having failed to get hold of the system specifications for the system acquired by the Office of the Prime Minister, the researcher concluded after reading the vendors document (Beijing CA-China Software Technology Co., Ltd. [2001]) on the system that this is a commercial off-the-shelf (COTS) system which many authors (Bantin 2002; Barry 1994; Fernandez and Sprehe 2003) caution against as they hardly have enough records keeping functionalities to support ERMS. As electronic records originate from the organisation’s existing or legacy information and communication technologies, ERMS should be

designed to suit a specific organisation in order to “create reliable and authentic records that provide evidence of critical activities of the institution” (Bantin 2002: 6). Implementation of an ERMS would be one of the important components of a records management programme for the Public Service of Namibia in the context of e-government. However, implementation of an ERMS would need to take into consideration the other systems that are running in the Public Service of Namibia and address the issues of interoperability.

Interoperability, accessibility and readability of electronic information over time

In response to the question, “How is compatibility of systems and exchange of data ensured?” the IT officer in Ministry B responded, “All systems are developed in different languages. It has not been tested if the systems are compatible. Everyone is running theirs separately. We would need to ensure compatibility and exchanges of data especially when we create an information management system bringing information from all databases”. The IT Officer in Ministry A responded, “For most systems the language is proprietary. For all future developments it will be content management systems, it will be web-based, in Oracle. All will be integrated”. The system acquired by the Public Service e-Office for electronic records management, with archives management, work flow and document management modules, seems to confirm this statement. An officer in the Office of the Prime Minister confirmed that e-Office was “tested to ensure that it can integrate with the Integrated Finance Management System and the Human Resources Information Management System. The idea is to integrate all these systems into this system”. Karjalainen *et al*., (as cited in Asproth 2005) established in their study that Enterprise Document Management Systems can provide a holistic solution for addressing technological and organisational problems associated with managing an organization’s information resources.

There were indications that the public service of Namibia is moving towards content management solutions. This is an effective way to provide online services or share information and transactions horizontally in support of e-government (Forquer, Jelinski and Jenkins 2005). As the study showed, without an effort on the part of the Public Service of Namibia to ensure compatibility of the different electronic information systems, enterprise content management will be difficult

to implement. Ngulube and Tafor (2006: 71) discussed the need for records managers in the Eastern and Southern Africa Branch of the International Council on Archives (ESARBICA) region to formulate policies and guidelines for "capturing of web-based records into formal records keeping systems". Electronic records management's place in enterprise content management is its ability to "tightly integrate with e-mail; document; and web content management systems to ensure content integrity and to minimize risk and litigation" (Glazer, Jenkins and Schaper 2005).

Systems documentation

Most of the institutions did not have the documentation of the electronic information systems which were running in their institutions. The private companies that installed the systems kept the documentation. Table 1 highlights the situation regarding system documentation.

Table 1: Systems Documentation

Institution	**Kept by the institution**	**Remarks by IT Officer/or specific officers using the systems**
Ministry A	Y/N	"We don't have a lot of documentation. I have for hardware. The … [One of the systems] was developed a long time ago in the 1990s and it has no documentation".
Ministry B	Y/N	"We don't have a central place where we keep it. I have tried to collect it but it is not comprehensive" (IT Officer). "Some of the changes are in people's heads. If we could get off the shelf application it would be much easier" (Officer in charge of one of the systems developed in-house by the Directorates).
Ministry C	N	"There is nothing".
Ministry D	N	"No system documentation".
Ministry E	N	"No documentation on how system was designed. Only procedures manuals".
Ministry G	Y/N	One system – "Yes we have it here". Another system – "What I have is outdated as

		there have been system upgrades. All up to date documentation is with the programmer in Pretoria".
Regional Council A	N	No system documentation. It is kept with the Windhoek Company that designed the system.
Regional Council B	N	No system documentation. It is kept with the Windhoek Company that designed the system.
Local Authority A	N	"Kept by the Consultant in Pretoria".
Local Authority B	Y	"Kept by the person responsible for standards and policies".

Y=Yes N=No

Digital preservation strategies rely on documentation for migration, emulation or any other strategies to ensure accessibility and readability over time; as well as overall effective management of electronic records. As Bearman and Trant (1997: 3) point out, "any record will be a better record (less risky) for having complete metadata". Responses to questions on the systems metadata standards and the data formats revealed that either these did not exist or if they did, they were not considered important.

The situation established by the study and discussed here signifies a great threat to the preservation of evidence from the records produced by the systems. A lack of metadata affects the readability and intelligibility of the information. Should the *Use of Electronic Communications and Transactions Bill* (Office of the Prime Minister 2005) be enacted, the Public Service would need to pay attention to preservation of system documentation and metadata to adhere to Sections 12, 13 and 14 which demand the preservation of authentic records. These sections among other things require that electronic records should be reliable, accessible and usable; and be retained in their original format or demonstrate that the current format represents the information accurately.

System upgrades

System upgrades were done on some systems in all surveyed institutions. The researchers wanted to investigate the impact the upgrades had on data and the structure of records. The IT officers

explained the move from the old finance management system to the new system, as well as the move from the old SQL human resources management system to the web-based Human Resources Information Management System. Cases of changes in data format and failure to access data with the new software or hardware were reported by some officers. This shows that “records created and maintained in electronic form are continually at risk of inadvertent or intentional alteration, and such alteration may not be readily perceptible. The authenticity of electronic records is threatened whenever the records are transmitted across space (i.e. when sent between persons, systems or applications) or time (when stored offline), or when the hardware or software used to process, communicate, or maintain them is upgraded or replaced” (National Archives n. d.).

An IT officer acknowledged that systems had not been tested for data loss or alteration and another officer explained that “alteration may not be readily perceptible”. This study did not notice any effort on the part of the public service of Namibia to ensure the authenticity of electronic records by verifying that the right data was properly stored; nothing happened to change this data or that the migration process was carried out correctly to ensure the reproduction of authentic records (Duranti and Thibodeau 2001: 49).

System safety and security

Various measures were described by IT officers on how safety and security is ensured. However, it was revealed that there was not much protection from the dangers that a fire outbreak might cause. That was evident from the various responses. “In the case of power failure … we have a redundancy in our server, a mirror system, as opposed to primary domain. If the primary domain goes out the mirror will take over. If they both go out we would need to reinstall a back-up” (Ministry F). The researchers established that the same system in Ministry D: “We have the mirroring system which mirrors all data from the primary disk to the secondary disk”. However, in both cases the primary domain and the mirror were kept in the same place so in the event of a fire both would be destroyed. The IT officer explained that “The ideal situation would be a duplicate main frame offsite”. The ministry did not do back-ups on tapes due to the non-availability of streamer tapes. “We have been struggling to get streamer tapes. If a

fire happens we are in trouble as we cannot do back-ups on tapes and store them off-site".

Asked if viruses threaten the system, one IT officer responded: "One of the Ministries, their anti-virus is not working so we spend time taking out viruses and reformatting". When asked what the impact was the response was, "They do lose data. It has happened to me". When asked if electronic documents lost always have hard copies as back-up, the response was, "It depends. If it's one which needed the PS's [Permanent Secretary] signature yes, but we don't print everything that is on computer". This problem of viruses corrupting data was established in other institutions as well. The system established reliance on electronic copies when hard copies cannot be found. This is common and it is not surprising considering the poor filing practices. It was also established that in some cases hard copies never existed in the first place, as it is not everything that is printed. However, as the next section shows, back-ups are not properly done and stored.

Furthermore, the use of non-official email systems due to inadequate bandwidth and inadequate storage capacity resulted in official information being kept in non-secure domains. The problems of security identified highlighted here have serious implications for the creation and preservation of trustworthy records. Viruses can corrupt records making them unreliable, or result in their total loss. Unsecure domains can result in records being manipulated.

Back-up practices

The research established several back-up practices. There were no standard back-up procedures in the Public Service and these practices were far from being satisfactory. As highlighted in Table 2 there were cases where officers' work was not saved on the server at all. There were problems of information not being found on the server where it is supposed to be for one reason or another. Some Ministries carried out some back-ups on the same server and where there were secondary servers for back-up they are stored in the same room as the primary server. One officer explained the Public Service policy regarding back-up storage media. "According to policy they [back-up tapes] were not supposed to be in the building. We are supposed to have a data bank where I am supposed to take them. For now I take

them home". The practice of keeping back-up tapes at home was found in three other institutions. Ministries in general did incremental back-up daily, weekly. Of all the institutions that performed back-ups on tapes, only one said that they did not overwrite tapes. Forty-eight surveys carried out by the National Archives of Namibia in central government, regional councils, local authorities and parastatals confirm these findings. However, all eight parastatals had off-site storage for their back-ups. None of the institutions studied had back-up guidelines for staff.

Poor back-up practices as established by the study pose a huge threat to preservation of evidence. The existence of back-ups stored at home was known by individuals concerned. In the event that anything untimely happened to them, these records may be lost to the institutions. The case of the Municipality of Omaruru which lost all its valuable data due absence of back-ups as reported in a local paper by Maletsky (2006) can happen to any of these institutions. Poor back-up practices signify that records meant to provide evidence in the Public Service of Namibia are at great risk of loss.

Table 2: Back-up practices at institutional level

Institution	Server/Other medium	Storage of back-ups	Remarks
Ministry A	Server and tapes	Off-site	"All documents are stored on the server with back-up off-site".
Ministry B	Mostly server and tapes as well for some of the systems	Off-site	Most of the in-house created databases rely on the automatic back-up done by the server. However some systems do back-up on tapes as well which are stored

			off-site. For one of the systems, the back-up tapes are kept at home by the officer in charge.
Ministry C	Server	Onsite	“We do back-up on the same hard drive. If it is damaged everything will be lost. All documents created by the officers are not backed-up on the server”.
Ministry D	Server and tapes	Off-site	Nil.
Ministry E	Server and tapes.	Onsite	The Ministry is in three buildings. Head office has no server so no back-ups are done. The other building has no network, so back-up is done for only one building. The tapes are stored in the same place as the server.
Ministry F			Does not have systems other than those maintained by Ministry of Finance and Office of the Prime Minister.
Ministry G	Primary server and	On-site	The Ministry has failed to secure

	secondary server		streamer tapes so it cannot do back-up on tapes.
Regional Council A	Server and tapes	On-site	"We have a server which is in a sort of safe place. Back-ups are done daily and then kept in safe place". The researcher observed that the tapes are kept in the same room with the server.
Regional Council B	Server and tapes	Off-site	Officer in charge keeps them at home.
Local Authority A	Primary Server and secondary server	Off-site	Kept by the company which set up and maintains the system.
Local Authority B	Server and tapes	Off-site	"IT Department does all the back-up. Individuals can also do if they wish".

Conclusions and recommendations

The many technological problems discussed in this article hampered the effective creation, sharing and maintenance of trustworthy electronic records. The study discovered that none of the electronic information systems which were running in the public service of Namibia had any records keeping functionalities. Implementation of an ERMS acquired by the Office of the Prime Minister might experience difficulties. Contrary to best practices there seem not to have been much of the required collaboration and cooperation between the National Archives (records management professionals)

and Office of the Prime Minister (IT professionals) in the acquisition of the ERMS.

The following are some of the recommendations focusing on addressing the technological problems identified by the study, aimed at strengthening the electronic records environment in the public service of Namibia.

- The public service should develop a “Policy on the Management of Government Information”. Other polices which also need to be developed, such as records management incorporating electronic records, e-mail policy, and enterprise content management policy will make this policy a point of reference. Such a policy will spell out the roles of the different stakeholders in the management of electronic records, such as the Office of the Prime Minister’s role in providing IT support and the National Archives’ role in providing the professional guidance in all matters relating to the management of electronic records.

- Preservation of system documentation for the electronic systems currently in the Public Service requires attention. The Public Service Information Technology Policy should have a statement on this.

- The public service needs to compile a database of all the electronic information systems running, capturing information such as metadata standards as well as other pertinent information. This could be done at Ministerial and Departmental level.

- To enhance the safety and security of records, a number of measures need to be put in place. Back-up procedures and management of back-ups need to be improved, the problem of virus attacks addressed and fire fighting equipment such as extinguishers and fire hoses provided not only for the registry but so that these be easily accessible to any office in view of the “mini” registries situation. The fire fighting equipment also requires regular servicing.

- Public Service Information Technology Policy could have a statement on electronic records management highlighting the

fact that records resulting from ICTs such as e-mail constitute evidence of government activities.

- Training for all members of staff in managing records has always been necessary, however with the shift of control of information management to individuals due to the use of certain ICTs, such training has become crucial.

- The creation of records centres, ideally one in each region, should be given serious consideration. In addition to relieving congestion in the offices through deposit of the paper records, records centres will provide the much needed offsite storage for back-up media.

Conclusion

The study established that the creation and preservation of trustworthy records in the public service of Namibia was threatened by technological problems. Technological problems needed not be viewed as the "usual" IT problems but serious problems affecting the creation and preservation of trustworthy records to enhance transparency and accountability. The public service of Namibia was at high risk of losing its corporate memory and evidence. Adequate resources for back-up, storage capacity, and improving systems security against virus attacks, loss in the event of disasters such a fire, and attending to issues of compatibility, and addressing inadequate bandwidth, were all measures necessary to ensure the reliability, authenticity, integrity, and usability of records in the public service of Namibia.

References

Amadeus International. n. d. Surviving the regulatory "perfect storm*".* [Online]. Available WWW: http://www.amadeussolutions.com/english/practices/bp_e_record.htm (Accessed October 6 October 2008).

Asproth, V. 2005. Information technology challenges for long-term preservation of electronic information. *International Journal of Public Information Systems* 2005 (1): 23-37.

Bantin, P. C. 2002. Records management in a digital world.

EDUCAUSE Centre for Applied Research Bulletin 16*.* [Online]. Available WWW: http://www.educause.edu/ecar/ (Accessed 23 March 2006).

Barry, R. E. 1994. *Towards a methodology for requirements definition*. [Online] Available WWW: http://www.caldeson.com/RIMOS/barry1.html (Accessed 23 March 2006).

Bearman, D. and Trant, J. 1997. A report from the archives community. A report of the 1997 Electronic Records Research Working Meeting. *D-Lib Magazine* July/August). [Online]. Available WWW: http://www.dlib.org/dlib/july97/07bearman.html (Accessed 2 October 2005).

Beijing CA-China Software Technology Co., Ltd. 2001. E-Office. Beijing: Author

Department of Defence. 2002. *Design Criteria Standard for Electronic Records Management Software.* U.S.: Author. [Online] Available WWW: http://jitc.fhu.disa.mil/recmgt/p50152s2.pdf (Accessed 5 September 2005).

Duff, W. 2001. Special issue: authenticity, social accountability, and trust with electronic records. *The Information Society* 17(4). [Online]. Available WWW: http://www.indiana.edu/~tisj/readers/full-text/17-4-guest.html (Accessed 30 March 2009).

Duranti, L. and Thibodeau, K. 2001. The InterPARES International Research Project. *The Information Management Journal* January: 44-50.

Erlandsson, A. 1996. *Electronic records management: a literature review*. ICA Studies 10. Paris: International Council on Archives.

Fernandez, L., and Sprehe, T. J. 2003. Integrating an ERDMS in an IT environment. *The Information Management Journal* July/August: 58-65.

Flynn, S. J. A. 2001. The records continuum model in context and its implications for archival practice. *Journal of the Society of Archivists* 22 (1): 79-93.

Forquer, B., Jelinski, P and Jenkins, T. 2005. *Enterprise content management solutions*. Waterloo, Ontario: Open Text Corporation.

Ghetu, M. 2004, May/June. Two professions, one goal. *The Information Management Journal:* 62-66.

Glazer, D., Jenkins, T and Schaper, H. 2005. *Enterprise content management technology*. Waterloo, Ontario: Open Text Corporation.

Gibbs, R. and Heazlewood, J. 1999. Electronic records: problem solved? *The Journal of the Australian Society of Archivists* 27(1): 1-13.

International Organisation for Standardisation. 2001. *ISO 15489-1 Information and documentation-records management-part 1 general*. Geneva: Author.

InterPARES Project. n. d. *Authenticity Task Force report.* [Online]. Available WWW: http://www.interpares.org/display_file.cfm?doc=ip1_report.pdf (Accessed 19 February 2005).

Jackson, R. 2008. *Record keeping standards confuse users, vendors*. [Online]. Available WWW: http://computerworld.co.za/news.nsf (Accessed 1 February 2008).

Keakopa, S. M. 2007. Management of electronic mail: a challenge for archivists and records managers in Botswana, Namibia and South Africa*.* Paper read at the XIX Biennial General Conference of the East and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) on *Empowering Society with Information: The Role of Archives and Records as Tools of Accountability,* in Dar es Salaam, Tanzania, 18-22 June, 2001.

Lipchack, A and McDonald, J. 2003. *Discussion paper.* Paper presented during the electronic discussion on Electronic Government and Electronic Records: E-records Readiness and Capacity Building, November/December 2003. [Online]. Available from WWW: http://www.irmt.org/download/DOCUME%7E1/GLOBAL/discussionpaper.pdf (Accessed 23 August 2004).

Maletsky, C. 2006. Computer theft paralyses Omaruru. *The Namibian,* November 18*).* [Online]. Available WWW: http://www.namibian.com.na/2006/November/national/065A605530.html (Accessed 17 November 2006.

Meijer, A. 2001. Electronic records management and public accountability: Beyond an instrumental approach. *The Information Society* 17: 259-270.

Moloi, J. 2007. E-records readiness in the public sector in Botswana. Paper read at the XIX Biennial General Conference of the East

and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) on *Empowering Society with Information: The Role of Archives and Records as Tools of Accountability*, in Dar es Salaam, Tanzania, 18-22 June, 2001.

National Archives. n. d. *Generic requirements for sustaining electronic information overtime: Defining the characteristics for authentic records.* [Online]. United Kingdom: The National Archives. Available WWW: http://www.archives.gov.uk/electronicrecords/pdf (Accessed 14 August 2006).

National Archives of Namibia. 2007. Namibia Country Report 2005-2007. Read at the XIX Biennial General Conference of the East and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) on *Empowering Society with Information: the Role of Archives and Records as Tools of Accountability*, Dar es Salaam, Tanzania, 18-22 June, 2007.

Ngulube, P. and Tafor V. F. 2006. The management of public sector records in the member countries of ESARBICA. *Journal of the Society of Archivists* 27(1): 57-83.

Office of the Prime Minister. 2005. *Use of Electronic Communications and Transactions Draft Bill*. Windhoek, Namibia: Author.

O'Shea, G. 1996. Keeping electronic records: Issues and strategies. *Provenance the electronic magazine* 1 (2). [Online]. Available WWW: http://www.netpac.com/provenance/vol11/no2/features/erecs2a.htm (Accessed 17 February 2005).

Sannet, S and Park, E. 1999. Authenticity as a requirement of preserving digital data and records. *ASSIST Quarterly,* Winter*:* 15-18.

Sejane, L. 2005. *An investigation into the management of electronic records in the Public Service in Lesotho*. M.A. Thesis. Pieter-maritzburg: University of KwaZulu-Natal.