British Journal of Economics, Management & Trade
10(1): 1-10, 2015, Article no.BJEMT.15460
ISSN: 2278-098X

SCIENCEDOMAIN *international*
www.sciencedomain.org

An Assessment of the Effectiveness of Electronic Records Management at Africa University, Mutare, Zimbabwe

Stanislas Bigirimana[1*], Nelson Jagero[2] and Pedia Chizema[3]

[1]Faculty of Management and Administration, Africa University, PO BOX 1320 Mutare, Zimbabwe.
[2]Faculty of Human Resource Development and Education, Chuka University, PO BOX 109 Chuka, Kenya.
[3]Department of Information and Communication Technology (ICT), Africa University, PO BOX 1320 Mutare, Zimbabwe.

Authors' contributions

This work was carried out in collaboration between all authors. Author PC did the research designed, data collection and wrote a much longer manuscript on electronic data maintenance. Author SB wrote the original manuscript while author NJ reviewed. All authors agreed that the study should be broadened to electronic data management rather than "maintenance" and additional literature review was done by author SB while author NJ provided insights on methodological changes needed to suit the new topic and reviewed various versions of the manuscript.

Article Information

DOI: 10.9734/BJEMT/2015/15460
Editor(s):
(1) Polona Tominc, Department of Quantitative Economic Analysis, University of Maribor, Slovenia.
Reviewers:
(1) Anonymous, Universiti Sains Malaysia, Malaysia.
(2) Regaieg Essafi Raida, Higher Institute of Management, Tunisia.
(3) Anonymous, Tianjin Chengjian University, China.
Complete Peer review History: http://sciencedomain.org/review-history/10644

Original Research Article

Received 26th November 2014
Accepted 7th August 2015
Published 23rd August 2015

ABSTRACT

The purpose of this study was to assess the effectiveness of the management of electronic records at Africa University. Effective management of electronic records implies effective creation, distribution, use, storage, securing, backup, and disaster recovery systems and procedures. At Africa University three departments, namely, the library, the accounts office and The Information and Communication Technologies (ICTs) Department are directly concerned with the maintenance of electronic records. Questionnaires were distributed to 14 employees from these three departments (from a population of 33 employees) while in depth interviews were conducted with

**Corresponding author: E-mail: sbigirimanaus@yahoo.com;*

the heads of these department, namely, the Bursar, the Librarian and the ICT Director. Responses indicated that maintenance of electronic records at Africa University is not effective.

Keywords: Electronic records maintenance; storage; backup; disaster recovery.

1. INTRODUCTION

This paper aims at assessing how effective are ERM systems and procedures at Africa University. Africa University is the first fully accredited United Methodist-related institution of higher learning on the African continent. It was established by the action of the United Methodist General Conference in 1992. According to the Africa University Prospectus, 2005-2007 [1]. Moreover, Africa University is the first private university in Zimbabwe Africa University is located in the Eastern Highlands of Zimbabwe, in a city called Mutare.

1.1 Formulation of the Problem

Taking advantage of the unprecedented development and diffusion of electronic computers and related Information and Communication Technologies (ICTs) Africa University has automated some of its operations. This implies that at Africa University volumes of electronic records are created on a daily basis. Africa University electronic records are stored at the ICT Server Room. These records include the university library electronic resources, accounts transactions, student records and all university ICT software. However, little is known on the strengths and weaknesses of current electronic records maintenance systems and procedures at Africa Universities especially in the areas of storage, security, disaster preparedness and policies and procedures. This paper aims at filling this knowledge gap.

2. LITERATURE REVIEW

According to Johnston and Bowen [2] electronic record maintenance implies 'the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities. Bearman [3] has pointed out that llike the maintenance of paper records, the maintenance of electronic records depends on their use. Duranti [4] highlighted that there are many types of storage media for electronic records, namely, magnetic media, optical disks, CD-ROM, and DVD. Magnetic media, commonly used for storage of state records, include hard disks, external drives, and magnetic tape. Currently, there are also USB memory sticks. Electronic records can either be stored in network-attached storage devices such as CD/DVD-ROM towers and in separate storage area networks. The United Nations [5] is of opinion that [w]hichever method chosen; the following should be kept in mind when constructing a storage system":

- Prevent data loss
- Offer adequate capacity that can easily be increased as storage needs grow
- Provide fast access to data without interruptions
- Be prepared for equipment failures
- Use cost-effective technologies

Record management implies a series of activities which include the creation, distribution, use, maintenance and disposition of recorded information maintained as evidence of business transactions [6] The common strategies in ERM includes (1) assigning unique identifiers to individual records, (2) protecting the records from unauthorised changes, and (3) maintaining audit trails which show how current records have evolved and the changes that have been effected [6].

An effective ERM systems ensures that the movement and location of records are controlled in a way that any record can be retrieved when needed and that there is an auditable trail of recordable transactions [7]. Therefore, storage accommodation for the records should be clean, tidy and secure. This prevents the damage to the records and provide a safe working environment for the staff. Furthermore, there is a need for planning for disaster recovery through backup and migration to new platforms [7]. Moreover, there should be archiving policies and procedures which meet the twofold aim of preserving important information and keeping it safe and confidential and at the same time making the information easily accessible when needed [7].

Confidentiality and accessibility can concurrently be achieved through proper classification, labelling and indexing files and file naming. The National Archives of Australia [8] defines records

classification system as a means of knowing what records exist and where they are kept in an organisation. It also facilitates easy access to records. Raas [9] laments that without a proper classification system in place a governmental body will not be able to obtain a disposal authority. This will prevent the timeouts disposal of records, which will in the long run have financial implications. Without a disposal authority in place all electronic records created will have to be migrated across changes in technology to enable them to be readable over a long period of time. National Archives of Australia [8] clearly reiterates that, "proper classification system management requires that there should be strict control over making additions to the directory structure or deleting folders from the structure". Adding folders randomly increases the risk of duplication. This can cause confusion when one wants to locate these folders. Deleting folders is a disposal action, which should only be allocated to the records manager/systems administrator. Because of the need to keep records of changes that have been effected in the filing, classification and disposal systems, The National Archives of Australia [8] suggests that records management software that provides for embedded filing might be the best choice. Therefore embedded filing happens for example when the user clicks the send button when sending e-mail and the user is automatically invited to file the message to the classification system in the repository. Preferably, the records management software that is chosen should provide the same embedded facility for all documents that are created electronically. If users are prompted as part of the normal procedure to file to the classification system in the repository when they save a document they might not even notice that they are managing records.

Seongwook and McLeod [10] define document classification as the process of selecting the appropriate subject from the classification system, and assigning the subject identifier to a specific document. This way all documents are associated with a subject in the classification system. This should preferably be an end user task. The National Archives of Australia [8] highlighted that iff the end users send documents to the repository without classifying them first, the systems administrator/records manager will have to review all documents sent to the repository and classify them in order to create proper records. Without being assigned subjects, documents that are supposed to be linked together and read in context will not be able to be retrieved as a single unit. It is so that powerful retrieval tools exist whereby records can be retrieved by using key word searches. However, practical experience has shown that if the correct key word is not used, records are not retrieved the results of the key word retrieval are so enormous that it takes up a lot of time to page through everything to find the documents that belong together.

Roper [11] highlighted that classification is required in order for disposal instructions and retention periods to be allocated and classification links paper-based records to electronic equivalents. It is very important that the paper-based records and the electronic records be classified against the same filing plan. This will ensure that records on a given subject in all media are managed against the same retention rules and that all records on a given subject are retrieved comprehensively.

In addition to classification, proper electronic records management includes labelling, naming conventions and indexing. The National Archives of Australia [8] defines "labels as essential to identify electronic media. Labels on a diskette's jacket (external labels) should include the originating office symbol, title, beginning and ending dates, what software was used to create the records (e.g., Mescal or MSWord), and on what equipment it was produced." The Government of New South Wales [12] says "labels on a computer magnetic tape should include the volume/serial number, the name of the office that created the data, and data set name(s)". Identification of any access restrictions should be included on any external label. Document, file and directory naming conventions (internal labels) should be easily understandable and standardised so that authors and their colleagues or successors can find and use information stored on disks or tapes.

According to National Archives of Australia [8] the purpose of naming conventions is that they are particularly useful when several people share a computer with a hard disk if the disk has not been partitioned into individual work directories. Labeling, naming, and filing conventions should be simple. One effective system is to file similar documents in the same place (on the same labeled floppy or in the same directory on a hard disk). This avoids the necessity of rummaging through a drawer full of diskettes or searching

through multiple directories on a hard disk to find needed documents.

National Archives of Australia [8] reviewed that indexing is a more complicated way to find an electronic document if a classification system is not used. Therefore adding that indexing system should require the document creator to indicate the name of the document, the addressee, the date, and the identifier of the disk on which it is stored. An abstract of the document may also be useful. The index can be printed out, or stored on cards or in a data base management system on a labelled diskette. Mutiti [13] is of idea that there is need to establish a formal, office-wide system for filing, labeling, and naming electronic records depends on how the information is used. Such a system is essential if the office plans to maintain records solely in electronic form, without converting the information to paper or microforms. Such a system is essential if the office plans to maintain records solely in electronic form, without converting the information to paper or microforms. If there is a high turnover of personnel, or if information is shared or routed electronically, a formal system may be particularly advantageous. If information is shared on paper, however, minimal identifying information should be sufficient.

Asogwa [14] observed that paper and electronic records maintenance systems should contain metadata (descriptive and technical documentation) to enable the system and the records to be understood and to be operated efficiently, and to provide an administrative context for effective management of the records. The record-keeping system, whether paper or electronic, should include a set of rules for referencing, titling, indexing and, if appropriate, security marking of records. These should be easily understood and should enable the efficient retrieval of information.

Policy development has been emphasised by many authors as key to good records management [15]. Such a policy would clearly set out the organisation's expectations regarding retention, individual roles and responsibilities, ownership, control, classification of different categories of content and privacy. [16] The failure to capture and preserve electronic records in eastern and southern African institutions of higher education have been attributed to lack of policies and procedures, among other factors [17].

Norris [18] reports that not many higher education institutions in the United Kingdom had well defined and active e-mail archiving policies in place. In fact findings from Duke University show that lack of defined policies resulted in different capabilities and different levels of e-mail management, backup, security and privacy usage among faculties [19]. Similar problems have been reported at Loughborough University [18] and at the University of KwaZulu-Natalu [20]. Therefore at Africa University should have proper policies and procedures that are well defined in order to preserve institutional e-records.

Myler and Broadbent [21] highlighted that once policies have been established the roles and responsibility of each individual in the organisation needs to be clearly set out and efforts must be made to ensure that everyone involved understands their roles and responsibilities thoroughly for instance, an individual using e-mail would be expected to identify and categorise e-mail records of value, apply consistently relevant contextual information and metadata, and ensure their integrity. The institution on the other hand has the responsibility of providing guidance on categories of e-mail to be retained and retention schedules, provide viable mechanisms for archiving of records, training and support to staff and students. Norris [18] emphasizes the duty of care whereby consideration needs to be given to how people do their jobs, how authority is delegated and the separation of responsibilities to reduce collusion and potential fraud.

According Harris [22] electronic records maintenance at universities should operate within the framework of policies, rules and procedures that give guidance to practice. The purpose of clear policies and procedures is to provide an environment conducive to proper records maintenance. This is particularly important in an environment, such as the universities, where the responsibility for electronic records maintenance is distributed among the individual units with little or no centralized control. Therefore adherence to proper policies and procedures is essential to provide broad guidelines in which procedures may be developed in the operations of the organization

Robek and stephens [23] pointed out that “the standardization of clear policies and procedures is to be realized, and then proper controls must be applied to records during the different stages they pass through from creation to disposal”.

This ensures that records maintain their value as authentic evidence of activity throughout their life cycle. Therefore the existence of a policies and procedures is critical in an organization such as Africa University.

Another important aspect of electronic records management is disaster preparedness and recovevery. Benson and Clay [24] define disaster recovery as assuring that the applications and data can be recovered and restored in a reasonable timeframe to continue running the business and making patient data available if there is a disaster in the primary data centre. The Government of New South Wales [12] emphasised that it important for the universities to back up electronic records on a regular basis to safeguard against loss of information due to equipment malfunctions, human error, or other disaster. Disaster recovery back-up tapes or other media should be kept solely as a security precaution and are not intended to serve as a records retention tool. In the case of disaster, the back-up would be used to restore lost records.

The Government of New South Wales [12] highlighted that electronic records that have not met their retention should not be disposed of on the basis of the existence of a back-up. If for any reason (for instance, a disaster erases e-mails on an system server), the only existing copy of an item that has not met its retention period is on a back-up tape or other medium, the agency must ensure that the record on the back-up is maintained for the appropriate retention period. A back-up containing record copies or the only existing copies of records that have not passed their retention would have to be retained for the length of the longest unmet retention period. Preferably, the records should be restored to an accessible storage device from the back-up to ensure that the back-up is not used as a records retention tool. National Archives of Australia [8] reviewed that universities IT policies to establish, and adhere to, a regular cycle of back-up overwrites based on the agency's security and disaster recovery needs.

Mnjama [25] summarises the requirements of maintaining documentation of all agency systems that store electronic records as the best practice for both records management and information technology; often, but not always, the IT program maintains such documentation. Documentation does not necessarily have to be completely separate for each and every application, as long as it is sufficient to ensure preservation and access to all of the records for as long as they need to be maintained by the agency. Agency of Records Management and ICT staff should work together to ensure the development of up-to-date documentation for all agency electronic records systems that is adequate to specify all technical characteristics necessary for reading or processing the records and the timely, authorized disposition of records.

3. RESEARCH METHODOLOGY

3.1 Research Design

The researcher used a case study.

3.2 Population and Sampling Techniques

The total population was constituted by 33 employees from the library, the accounts office, and the Information and Communication Technologies (ICTs) department. A sample of 11 employees were purposefully selected based on their involvement in ERM on a daily basis. In addition to the 11 employees, in depth interviews were conducted with the heads of the respective departments. Data obtained from administering questionnaires to the employees and interviewing the heads of departments as organised thematically handling issues of data creation, distribution, use, storage, security, disaster recovery and policies and procedures. Table 1 shows the distribution of the population and the sample in various Africa University's departments.

3.3 Research Instruments and Data Collection Procedures

11 questionnaires were distributed to staff in the three selected departments while in depth interviews were respectively conducted with the Bursar, Librarian and ICT Director. Permission to conduct the research was sought for and granted in writing by the University Registrar.

4. FINDINGS AND PRESENTATION

4.1 Awareness of Electronic Records Maintenance Policies and Procedures

Fig. 1 shows that 8 (33, 4%) respondents indicated that there was electronic records maintenance policies and procedures. The highest number, 16 (66, 6%), indicated that there was no policies and procedures that are followed

in the maintenance of electronic records at Africa University.

Table 1. Table of sampled population

	Total population	Total sample
Heads of departments	3	3
Library staff	10	3
Accounts office staff	5	2
ICT staff	15	6
Total	33	14

From the interview it has been gathered policies and procedures are there but they are not always being followed by the staff owing to poor supervision. The problem, therefore, poor dissemination of information on electronic records policies and procedures. Concerning the importance of policies and procedures in the maintenance of electronic records. The majority, 20 (55, 6%) were of the view that these policies and procedures maintain the standards and guide electronic records administrators in the proper ways of maintaining the records. However only four (11, 1%) pointed to the fact that records will be preserved in maximum security.

4.2 Security Systems in Place for Protecting Electronic Records

From all the respondents, only (11) 44% respondents indicated that there are security systems in place for the electronic records while (14) 56% mentioned that there are no security systems in place. The results showed in Fig 2 demonstrate that the security systems of electronic records maintenance were unsatisfactory. When looking closely at these results, the researcher noted that there are security systems in place for safeguarding electronic records but there might be lack of information awareness to staff.

Table 2 reveals the reasons most respondents stated on the importance of security systems. 21% (3) staff indicated that security systems are important for limiting unauthorized access to electronic records, while 21% also cited that it is also important in daily backups of the systems so that records are not fraudulently altered. Security strategies including securing databases (28%) while keeping passwords sage (21%). 7% suggested that electronic records would be safer if there was a offsite back up system.

4.3 Security: Restrictions of the Access to the Sever Room

All respondents indicated that the restriction of access to the server room is a key security measure. From the interview with the ICT director, it was highlighted that staff who are authorized to enter the sever room have to use a log book that indicates the time they have entered the server room and the time they will be out. The ICT Director pointed out that restrictions of access to the sever room minimizes the

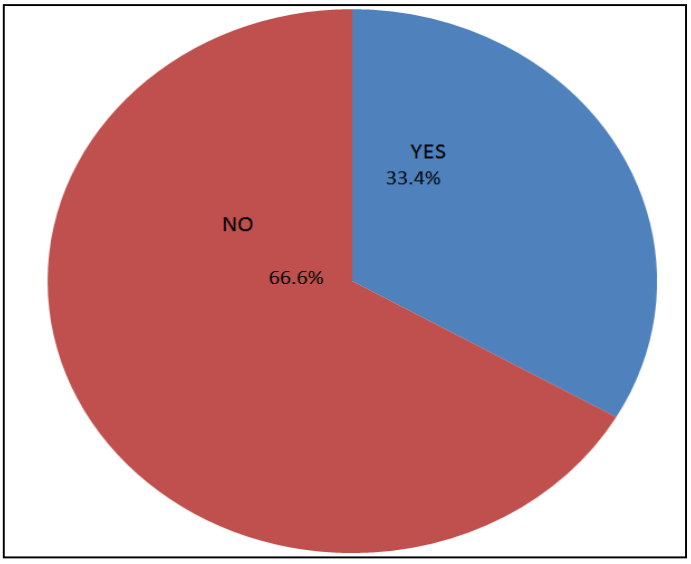

Fig. 1. Electronic records maintenance policies and procedures awareness

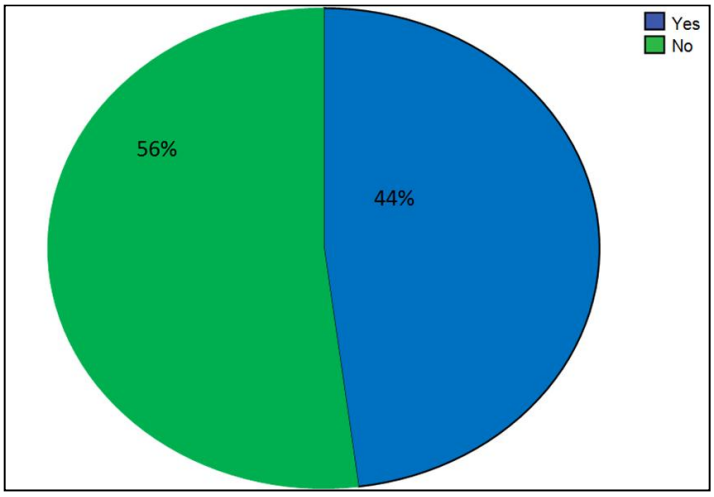

Fig. 2. Security systems in place for protecting electronic records

possibility of tempering with the servers by the unauthorised personnel and minimises the pilferage of electronic media. The University Librarian also highlighted that restriction of access to server room protects the confidentiality of records that contains vital institutional information. The Bursar highlighted that the restriction of access to the server room is crucial as it also protects media that contains financial and accounting records of the institutions and minimizes deletion of records either through human error or fraudulent activity. The ICT Director is aware of the crucial role his department has to play in the effective security of electronic records at the University. He indicated his willingness to implement a computerised security system of the sever room. From the questionnaire, the researcher noted that the staffs have knowledge on the security features for the server room restriction as the majority of them had cited different reasons for server room restrictions.

4.4 Backup of Electronic Records

As shown in Fig. 3 24% (6) of the respondents indicated that backup of electronic records is done every day, while 48% (12) indicated that backup is done weekly. The other 24% (6) indicated that they do back up monthly and 4% (1) has indicated that it is done yearly. From these results it showed that backup of electronic records seems not to be consistent. There is no written standard operating procedure for the backup of the electronic records that indicates the schedule for backup. Therefore there is need for supervision for all staff that are administering the maintenance of electronic records in order to come up with a proper back up policies and procedures that will be followed by all electronic records administrators.

4.5 Disaster Recovery Plan

As shown in Fig 4, three respondents (12%) indicated that Africa University have a disaster recovery plan to protect electronic records, while 40% (10) indicated that there is no disaster recovery plan and the other 48% (12) are not sure if there is a disaster recovery plan or not. Looking at the responses from interviews and the ones from other respondents, it might be clearly said that the institution does not have a Disaster

Table 2. The importance of security systems

Respondents suggestions	Frequency	Percent	Valid percent	Cumulative percent
Limited rights to electronic records	3	12.0	21.4	21.4
daily backups	3	12.0	21.4	42.9
database security	4	16.0	28.6	71.4
Safekeeping of passwords	3	12.0	21.4	92.9
Protecting of offsite backup media	1	4.0	7.1	100.0
Total	25	100.0		

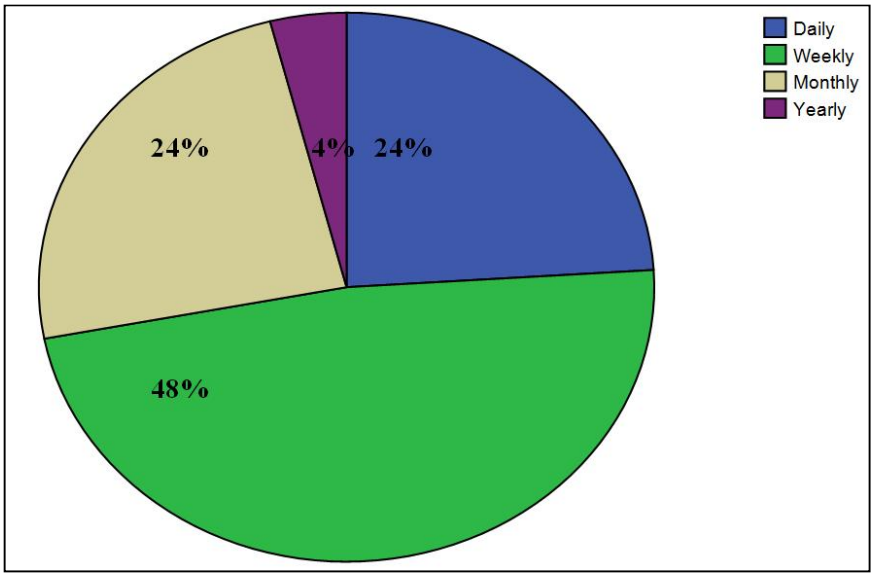

Fig. 3. Backup of electronic records

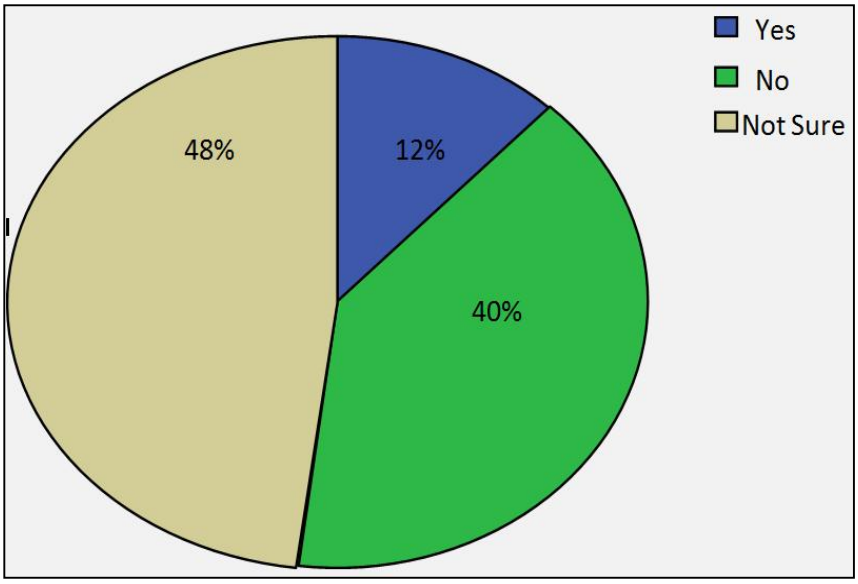

Fig. 4. Disaster recovery plan

Recovery Plan to protect electronic records. However, there might be a disaster recovery plan at Africa University but probably because it is not communicated to the staffs, most people might not be aware of its existence. This shows that there are limitations in the way the institution is disseminating information. Therefore, transparency in the way of disseminating information should be encouraged so to promote awareness at the institution.

5. CONCLUSION

The study revealed that there is no effective maintenance of electronic records at Africa University. Staffs are not aware of existing policies and procedures although access to the server room is restricted. The staffs are aware of the importance of security measures such as security databases, upholding passwords and keeping off site backup systems. However, at the

implementation level, are discrepancies in the regularity of backup which indicates that either there is clear policy or the policy which is not there is not consistently implemented. Most staff are not aware of the existence of a disaster recovery plan.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Africa University Prospectus (2005-2007), Mutare, Africa University Press; 2004.
2. Johnston P, Bowen D. The benefits of electronic record management systems: A general review of published and some unpublished cases. Records Management Journal. 2005;15(3):131-140.
3. Bearman D. Item level control and electronic recordkeeping. Archives and Museum Informatics. Cultural Heritage Informatics Quarterly. 1996;10(3).
4. Duranti Luciana, Terry Eastwood. Protecting electronic evidence: A progress report. Arclzivi & Conzputer 5. 1995;3.
5. United Nations, Management of Electronic Records: Issue and Guidelines. New York State Archives and Records Administration; 1990.
6. Available:http://www.aiim.org/What-is-ERM-Electronic-Records-Management (Accessed on 14 February 2015)
7. Available:http://www.dhsspsni.gov.uk/gmgr-4e (Accessed on the 14th February 2015)
8. National Archives of Australia Archives advice 24: Distributed Management of Electronic Records; 1998. Available:http://www.naa.gov.au (Accessed 19 September 2013)
9. Raas U. Electronic record keeping- more than electronic document management. Records Management Journal. 1999;9(2): 117-129.
10. Youn, Seongwook, McLeod, Dennis. A comparative study for email classification, advances and innovations in systems, computing sciences and software engineering. 2007;387-391.
11. Roper M (ed). Managing public sector records. A Study Programme. Managing Electronic Records, International Records Management Trust; 1999.
12. State Records NSW. Standard on Managing a Records Management Program. Standard No. 8; 2004.
13. Mutiti N. The challenges of managing electronic records in the ESARBICA Region, ESARBICA Journal. 2001;20: 57-61.
14. Asogwa BE. The readiness of universities in managing electronic record: A study of three federal universities in Nigeria. The Electronic Libraries; 2012.
15. Kahn RA. Records management & compliance: Making the connection. Information Management Journal. 2004; 38(3):28−36.
16. Myler E, Broadbent G. ISO 17799: Standard for security. Information Management Journal. 2006;40(6):43−52.
17. Wamukoya J, Mutula SM. Capacity-building requirements for e-records management: The case in east and southern Africa. Records Management Journal. 2005;15(2):71−79.
18. Norris M. Records management and e-mail; 2003. Available:http://www.dcc.ac.uk/events/ec-2006/EC_emailarch-rep.pdf (Accessed 18 September 2013). Page 14 of 15
19. Tibbo HR, Pyatt T. Email management, electronic records, and beyond; 2006. Available:http://www.ils.unc.edu/digitaldesktop (Accessed 17 September 2013)
20. Chinyemba A, Ngulube P. Managing records at higher education institutions: A case study of the university of KwaZulu-Natal, Pietermaritzburg Campus. South African. Journal of Information Management. 2005;7(1). Available:http://www.sajim.co.za/peer86.7nr1.asp. (Accessed 10 October 2013)
21. Myler E, Broadbent G. ISO 17799: standard for security. Information Management Journal. 2006;40(6):43−52.
22. Harris V. The challenges of preserving electronic memory over time. Paper read at Electronic Records Management Conference, Sandton, SA; 2003. Available:http://www.jisc.ac.uk/media/documents/publications/recordsmanbriefin (Accessed 30 September 2013)
23. Robek MF, Brown GF, Stephens DO. Information and records management: Document-Based information systems. New York: Glencoe/McGraw-Hill; 1995.
24. Benson Charlotte, Clay Edward. Understanding the Economic and Financial

Impacts of Natural Disasters, Washington D.C., The World Bank; 2004.
25. Mnjama NM. Managing university records. ESARBICA Journal: Journal of the Eastern and Southern Africa Regional Branch of the International Council on Archives. 2002;21:32-40.

© 2015 Bigirimana et al.; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/10644