DOI: 10.36347/sjebm.2016.v03i02.002

Scholars Journal of Economics, Business and Management e-ISSN 2348-5302
Naftal Chweya Oganga.; Sch J Econ Bus Manag, 2016; 3(2):64-72 p-ISSN 2348-8875

(An International Publisher for Academic and Scientific Resources)

Managing Records for Good Governance in E-Government Environment: The Kenya Experience

Naftal Chweya Oganga
Department of Library, Records Management and Information Studies, Moi University, Kenya

*Corresponding Author
Naftal Chweya Oganga
Email: nafcochweya@yahoo.com

Abstract: The government of Kenya like other Governments around the world is pursuing strategic objectives designed to enhance the effectiveness of government programmes and operations, promote good governance, transparency and accountability through the use of Information Communication Technologies (ICTs). This paper seeks to answer three basic questions. What is involved in managing electronic records in an e-government context? What are the risks of not managing e-records as a strategic public resource? What is the future of e-records management in Kenya? This paper is a review paper focusing on the situation in Kenya, drawing from other cases in Africa and other parts of the world.
Keywords: Good Governance, e-government, Electronic Records

Introduction

The emergence of Information and Communication Technologies (ICTs) have provided means for faster and better communication, efficient storage, retrieval, processing of data, exchange and utilization of information to its users, be they individuals, groups, businesses, organizations or governments. Information and communication technology (ICT) offers a powerful tool that, if deployed equitably, can ensure citizens are empowered and Government can deliver services more efficiently, effectively and in a transparent and accountable manner. Information is vital for the efficient delivery of public and private sector products and services that are responsive to the needs of citizens and businesses and key for capacity creation. The electronic delivery of services to business and the citizen will produce electronic records as evidence of individual transactions; this evidence will need to be retained and maintained over the medium to long term as records which can demonstrate accountability and preserve reliable access. The replacement of manual and paper-based processes with electronic processes in government administration will generate electronic records as evidence in policy-making, casework and service delivery areas.

Electronic records management and the e-government strategy

The electronic delivery of services to business and the citizen will produce electronic records as evidence of individual transactions; this evidence will need to be retained and maintained over the medium for long term use as records which can demonstrate accountability and preserve reliable access. Up to the present time, new information systems development often generates electronic records that do not fall under any formal corporate management and control. Effective electronic records management to support e-government will require a formalization of control over electronic records already existing in departments and agencies, as well as planning for those that will be generated by new service delivery and policy-making systems. Government organizations need to manage electronic records as valuable corporate information resources.

The International Records Management Trust (IRMT) developed a record readiness tool in 2002 to enable governments to conduct high-level assessments of key areas of e-records readiness in relation to other aspects of e-government and to determine whether the records and information management infrastructure is capable of supporting e-government initiatives [3]. The tool uses a brief questionnaire that provides a risk assessment of e-records readiness in government, at national and enterprise levels. The areas addressed by the tool include among others: staff competencies in maintaining software and hardware; human resource capacity; telecommunication infrastructure to support growing volume of work; adequacy of electric power; information management policies and responsibilities; information management products and technologies; internal and public awareness programme of information management; compliance with information management procedures such as security,

documentation standards and system engineering procedures for ICT; guidelines for management of electronic records; national ICT strategies; supportive legal and regulatory framework for information management; and freedom of information and protection of privacy.

Thirteen years later it is evident from the literature whether Government ministries in Kenya are using the IRMT tool. However, going by recent developments and a survey by IRMT in 2014 it would seem that by and large, the KNADS the statutory institution with responsibility for archives and records management in Kenya fall short of the e-readiness standards of the IRMT benchmarks. For example, staff competencies, skills and tools needed to manage e-business processes and e-information in a shared work environment has not been adequately developed in many public sector organizations in Kenya. Among records and information managers, and national archivists, there is insufficient capacity and training to articulate e-records issues and provide guidance and input to policy makers and planners. This situation is complicated further by the fact that at policy level, senior officials and legislators are often unaware of the requirement to manage electronic records over time so that the evidence base of government will be secure and accessible when needed by authorized users. At the planning and operational level, systems designers and IT specialists tend to focus primarily on current information needs resulting in inadequate attention being paid to long-term preservation requirements [3].

A study on *Aligning Records Management with ICT/ e-Government and Freedom of Information in East Africa* between February 2010 and September 2011, by the International Records Management Trust found out that records management issues are not being addressed in relation to the ICT/ e-government initiatives that are being planned and implemented within the region.

According to the study Kenya, Uganda, Tanzania and Rwanda have made substantial investments in ICT procurement and deployment. ICT plans are supported at the highest level of government, and while the agencies involved varied from country, there was significant senior level support. All of the EAC countries are moving forward aggressively to implement ICT plans, with e-government initiatives designed to harness the power of the Internet to deliver information and services more effectively to citizens [1].

Despite the profile of ICT/ e-government plans and the high level of importance being accorded their implementation, there was little evidence that any of the countries were addressing records management concerns as part of the planning process. Only in Tanzania has the National Archives been consulted in planning and developing ICT and e-government policies, strategies and projects. Generally, the archives and records authorities were not involved in government information management initiatives. The Kenya Government was implementing a digital document and records management system that was to be rolled out across the public service, but this was being spearheaded outside the Kenya National Archives and Documentation Service. Rwanda had adopted a document workflow management system, but it did not incorporate the full records management functionality. Records specialists from the archives and records authority had not been involved. Generally, the ICT systems being implemented had not been developed to take account of records management requirements. As a result, there was a high risk that digital records would not being captured and protected systematically [2].

The increasing use of ICT, especially the Internet, in government operations around the world driven by public service delivery, has given impetus to the generation of e-records, touted as strategic assets vital to the functions of the state. Like traditional paper records, e-records support the day-to-day operations of government services and interactions with citizens, private and public sector partners. By and large, in developed regions such as North America and Europe where government services have increasingly moved online, e-records are becoming the basis for confirming pension and other entitlements; registering births and deaths; verifying citizenship, certifying voting rights; enabling collection of taxes, supporting financial management; and supporting litigation [3].

Mnjama and Wamukoya[4] pointed out that there were real challenges faced by East and Southern Africa member countries in the capture and preservation of records. These include: absence of organizational plans for managing records; low awareness of the role of records management in support of organizational efficiency and accountability; lack of stewardship and coordination in handling records; absence of legislation, policies and procedures to guide the management of records; absence of core competencies in records and archives management; absence of budgets dedicated for records management; poor security and confidentiality controls; lack of records retention and disposal policies; and absence of migration strategies for records. These challenges will be more pronounced with the advent of electronic records management.

A case study undertaken by Akotia[5] in the Ministry of Finance in Uganda on the management of financial records in government established that

throughout the government of Uganda, ICT was considered an indispensable tool for enhancing productivity, yet little attention was paid to the electronic records management issues and to understanding the forces of change that affect the form and integrity of the record created within an IT environment.

Kemoni[6] also noted that government Ministries in Kenya had no capacity for managing the basic elements of an electronic records programme including: staff who understood the functional requirements for record keeping and had the competencies and skills required to manage electronic information delivery systems; legal and administrative requirements for managing electronic records; and accurately documented policies, standard operating procedures and formal methodologies for managing e-records.

The Government of Kenya has established a well developed structure of bodies and committees to facilitate e-Government Strategy. The institutional framework for e-Government includes a Cabinet Committee that oversees the implementation of Kenya's e-Government Strategy and a Permanent Secretaries' Committee, chaired by the Head of the Public Service, which is charged with co-ordinating the implementation of e-Government initiatives and providing institutional support to expedite e-Government implementation. There are also e-Government committees at the ministry level, chaired by the Principal secretary, that are responsible for auditing ICT capacity, identifying technical and institutional gaps and inadequacies, and making recommendations on the way forward.

The Directorate of e-Government, under the Head of Public Service in the President's Office, provides a technical steering team that serves as the e-Government Secretariat. The Secretariat is charged with preparing and co-ordinating the e-Government Strategy, including the implementation plan, and with monitoring and evaluating the process. The Directorate's agenda is set out in its 2009-2012 strategic plan and is driven by Vision 2030 as well as by government's priorities for land administration, immigration, the judiciary and birth, death and marriage registration. Although the management of electronic records does not yet feature as a key component of the e-Government agenda, the Kenya Communications (Amendment) Act, 2009 includes significant relevant provisions on electronic records. The Act defines e-Government services as those provided electronically by a ministry or government department, local authority or any body established by or under any law or controlled or funded by the Government, and it recognises the legal validity of electronic records as a means of facilitating electronic commerce. It deals at length with electronic records issues as essential to promoting e-Government and e-commerce. It gives electronic records legal recognition, authorises the use of electronic signatures, and addresses the need to manage public sector electronic records to ensure that they are authentic, secure and reliable records as a basis for efficient and effective service delivery. It requires the Communications Commissioner to ensure that electronic transactions are based on reliable electronic records. However, it does not stipulate requirements for capturing and managing authentic and reliable electronic records.

Policy and strategy for electronic records management

At present there is little infrastructure in government organizations for electronic records management. Government organizations will need to develop infrastructure for ERM by integrating ERM facilities and procedures into new e-government systems and business processes as these are developed and implemented, and by ensuring that electronic records are captured and made available for effective management in controlled records management systems as these become operational. Electronic records management runs across many technologies and underpins the sustainable establishment of electronic services. Such services will generate records, received from business, the citizen or generated by the departments dealing with the transactions, and these must be captured, retained and appropriately disposed of.

Although the Government of Kenya has put in place the National ICT Policy and E-Government Strategy that provides guidelines for transformation of the country into a digital society, the management of electronic records does not yet feature as a key component of e-government. The Government of Kenya has established a well developed structure of bodies and committees to facilitate ICT/ e-Government development. However, the issue of managing the electronic records produced by ICT applications has not yet been tackled systematically. A survey by Thurston revealed that the procurement of electronic records management systems was taking place within a number of public bodies without a standard policy or even a functional requirements standards have been adopted. There are therefore a multitude of systems across government ministries and departments. This will pose a lot of risks and dangers in recordkeeping as the preservation and management of records in such environment will not meet the basic recordkeeping requirements. The government of Kenya is yet to have a common approach towards the development of a

common model system on a national level for electronic records management.

Although, the Kenya National Archives and Documentation Service (KNADS) is the primary agency with legal responsibility for the management of public records, but its lay back approach in electronic records management is currently resulting to the department not recognised as having a role in managing electronic records, and other agencies are being assigned responsibilities for managing electronic records. The Kenya commission (Amendment) Act 2009 includes provisions that put the responsibilities of the management of electronic records under the Communication Commission of Kenya (CCK). The commission's duties overlap with those of KNADS, duplicating records management functions that have already been assigned to KNADS by the Public Archives and Documentation Service Act. Further, CCK does not consider KNADS relevant in the management of electronic records [7].

International good practice requires that a single authority should be vested with responsibility for the records management function from the point that records are created. The issue of allocating responsibility for the electronic records management function in Kenya need to be addressed as the country embraces the concept of e-government. In the electronic environment, it is essential to manage records from the point of creation, as they are at risk if they are not under continuous professional control and the phases of control cannot be separated and assigned to different agencies as might have been possible in the paper environment.

Skills and competencies for electronic records management

Mnjama[8] argue the KNADS is seen as a success story by many African archival institutions. The department has made major strides in developing records management services. However, as Wamukoya and Mutula[9] correctly assert the shift from paper to electronic records and digital information provides new challenges for records managers and archivists in terms of skills, expertise and training. A study by Kemoni[10] established that although the government of Kenya had adopted e-government concept the government was yet to develop guidelines and standard relating to the identification, storage, appraisal and disposition of electronic records.

KNADS which is expected to take a lead in advising government ministries and departments on how to manage electronic records is likely to be hampered by lack of technical know-how. For long the department has been expected to take deliberate actions to train its staff in IT and electronic records management.A survey by IRMT [11] established that although the KNADS had a large number of well-qualified records and information professionals, the largest cluster to be found anywhere in the Government only two of the staff had a Diploma in ICT. The KNADS staff has acquired some practical knowledge of electronic systems through personal initiatives, but they do not have experience of or in-depth training in the management of electronic records.

The emphasis in electronic records management shifts from direct management of the record as physical artifact towards design of the infrastructure in which the record is created, captured and managed by a mix of the individual end user, software systems, and management procedures. For KNADS this is likely to involve the acquisition of a new range of skills to manage new kinds of systems in new contexts. This involves the development of multi-skilled and multi-purpose project and operational teams, bringing together a range of different skills and expertise – some new and relatively untested. Responsibility rests here on the KNADS for developing record-keeping infrastructure, and providing guidance and training opportunities for the end user who creates and uses electronic records.

Kemoni [12]established that KNADS was taking some measures for capacity building on electronic records management by seconding its IT Officer to the University of Glasgow, from October, 2005 to January, 2006 under the Commonwealth Professional Fellowship Programme. The Officer was expected to develop a policy document and guideline for managing electronic records in the Kenyan public service. A resultsdid not reveal that this is yet to be done, nor did the knowledge and exposure acquired been shared with other archivists in the department.

The success of e-Government initiatives in Kenya as in other countries in the world will entirely depend on how electronic records are created and managed. The common denominator at the centre of e-government initiatives is the electronic records management. ICT systems will fail if electronic records cannot be identified, retrieved and used; if they are stored improperly; or if they cannot be linked to related paper records and metadata. E-government initiatives will fail and citizens' trust in government services will be eroded if the Government is unable to find the records that underpin these services or if citizens discover that the integrity, completeness and accuracy of the information in the records cannot be trusted.

E-Records Management in Kenya and its implications for governance

The importance of e-records management in Kenya's good governance and service delivery need not be over emphasized. Accurate and reliable records form the documentary evidence needed to provide a foundation for all government strategies. The loss of control of those records and information systems, particularly in electronic environments, is a highly significant global problem. In the electronic age, sound records management systems are critical to the public sector so as to be accountable and transparent as well as to improve services to citizens. Well-managed e-records systems provide a strong foundation for enhancing accountability, transparency, democratic governance, poverty eradication, elimination of corruption, and efficient use of donor-funded resources [13].

Increasingly, various activities within the Kenyan public service are generating vast amounts of electronic records that need to be properly managed in order to enhance transparency and accountability in the management of public affairs and in the effective delivery of services. Sound record keeping practices are increasingly being tied to enhanced performance, transparency and accountability in government. Governments play a central role in all elements of national society. The public sector is the principal factor in the macro socio-economic policy making and the key catalyst for national development. It has the responsibility for the planning, formulation and implementation of policies, programmes, and projects for the delivery of goods and services to the nation.

As governments make the transition from the traditional paper-based records management environment to ICTs, the emphasis has largely been on improving access to information and transaction-based services for the public, clients and partners. But ultimately, there is potential for restructuring and improving internal management and administrative processes such as policy formulation and implementation, development planning, service delivery, monitoring and evaluation; creating new governance partnerships involving different levels of government, the broader public sector and the private sector; reengineering the way major public sector systems such as health, justice, land, education, transportation and human resource are managed and how they function, thereby increasing efficiency and delivering a broader range of services; fostering digital democracy and increased citizen involvement in their own governance through two-way communication and feedback between citizens and the government [14].

E-government provides the opportunity for governments throughout the world to improve the delivery of information and services to citizens and businesses, to streamline public sector functions, and to increase citizen participation in government. In some instances this is just a matter of providing electronic access to existing information. In others, electronic services, such as land searches or submission of tax returns, are being delivered online. Electronic government has the potential to transcend constraints imposed by distance and increase the speed of service delivery, but it also poses a number of challenges for accountability, the rule of law and the maintenance of organizational memory. Furthermore, governments face increasing public pressure to demonstrate that they are accountable to their citizens and that they are committed to efforts to root out corruption or malpractice.

As more citizen/state interactions occur in electronic form, it is vital to ensure that electronic systems support evidentiary record keeping. Citizens will expect that their rights are as well protected and documented in an electronic environment as in a paper-based one. This can only be achieved if the records generated through the electronic government are carefully managed through systems providing constant intellectual and physical control. The aim must be to preserve the combination of content, context, and structure which give electronic records meaning over time, to protect the fragile media from degradation, and to ensure efficient access [15].

IRMT [16] points out that as e-government services are delivered using new ICTs, the intended benefits will be compromised unless there is an adequate infrastructure for managing the e-records that will be created. Traditional records and information management tools, such as classification schemes and disposal schedules are necessary to ensure that e-records are protected as reliable evidence. Failure to address these issues could lead to reduced government effectiveness; increased operating costs; gaps in recorded memory; reduced public access to entitlements; erosion of rights; and weakened capacity for decision making.

Chronic weaknesses in government record keeping can adversely affect private sector investment. For example, overseas firms may hesitate to invest in a country if they feel its courts do not handle civil cases (especially commercial cases)efficiently. Likewise, large-scale infrastructure investments, such as the construction of gas pipelines, may be delayed or may incur significant additional costs if government land registries cannot provide complete and definitive statements of titles to property. Poor record keeping can contribute to a lowering of the general standard of service offered to businesses. For example, there may be delays in replies to written inquiries about the registration of businesses, the issue of licenses, and

other matters necessary for companies to pursue their business.

Within an e-environment, the role and participation of the private sector is critical especially with regards to e-commerce and e-business transactions. In order to achieve this, governments need to provide a conducive environment through enabling legislations, and regulatory frameworks. As more and more private sector and government activities are carried out online in electronic format, such legislations and regulatory frameworks will be critical for ensuring the availability of reliable evidence of activities transacted to protect the rights, obligations and entitlements of all parties involved[17] observed that under existing legislation, courts around the world have struggled with applying the traditional rules of evidence to e-records with inconsistent results. In order to facilitate dispute resolution and avoidance, governments need to adopt laws that establish ground rules for e-transactions, e-commerce and the use of e-signatures.

Risks in relation to Electronic records management

The electronic delivery of services to business and the citizen in public sector is producing electronic records as evidence of individual transactions which need to be retained and maintained as evidence that can demonstrate accountability. In government, electronic records are public records and they must be subject to more stringent controls to protect their authenticity. According to [18] the authenticity of electronic records is threatened whenever they are transmitted across space, that is, when sent to an addressee or between systems or applications or time when they are in storage, or when the hardware or software used to store, process, communicate them is updated or replaced. It has become widely accepted that electronic records are at greatest risk of losing their "recordness" at moments when they are transitioning between states and when control is being passed to different systems [19].

It is possible to track every access to a records system and every action on any record in the system. A system can be designed so that, once filed, a record is never out of file; users get access only to copies of the record. System design can also preclude any alteration or destruction of records except by authorized persons. However, such controls are only effective within the confines of a system. When a record is taken out of a system, or when the system itself is modified, systematic control is at risk [20].

Various studies on electronic records carried out in the 1990s [21]According to these studies the life of an electronic record falls under the control of four discrete environments, namely; creation environment, active records management environment, archival environment and preservation environment. Within these four environments there are various occasions in the life of documents that are particularly risk for the integrity and authenticity of the record.

Creation Environment Risks

The first moment of risk in the life of an electronic record is at the moment of capture, where it is determined whether the records is saved in the creator's systems and captured in the recipient's system at all, or in the same form. A review of literature agreed that when a system creates data reflecting an institutional or individual action, and that data is captured by the sender or recipient in the course of a transaction or communication, a document of one or more files or data formats is created [22]. Technically, any created document can reside in RAM in the creating system and fail to be saved as a record, but a copy of it has to be recorded in the receiving system. To some, whether the document becomes a record depends on whether it is then set aside – that is, consciously managed – by the sender or recipient [23].

As the Inter PARES Project [24] put it, a record is defined as any document created – meaning made or received and set aside either for action or reference– by a physical or juridical person in the course of practical activity as an instrument or by-product of it. The act of capturing takes place within the sending system and the receiving system independently, but does not create something that must be managed as a record. In the sending system, the saving of a document (but not of a record) is, as a technical matter, essentially risk-free. But socially, saving a document can be very risky. The sender may dispose of it rather than setting it aside in a management system, or may change it, purposefully or accidentally, prior to setting it aside in a management system. The capture of the same document within the receiving system involves more risk.

Risks relating to Metadata

The largest risk faced by anyone using electronic information systems, and ultimately by records managers, archivists, and those concerned with evidence, is that documents are not, by anyone's standards, the same as records. In order to save a record, the captured document needs to be accompanied by adequate metadata relating to content, structure, and context to establish its value as evidence [25] further argue that both content and metadata need to remain together, unaltered, and usable over time. There is agreement in literature that systems do not necessarily make records and that there is a major risk, incurred at Capture and again at Ingest, that inadequate metadata may be captured or it might be stored in a way that permits it to be alienated from the record to which it

applies. In explaining the importance of metadata, [26] argued that, as records move beyond the boundaries of the local domain in which they were created or, as is increasingly the case in networked environments, they are created in the first place in a global rather than local domain … metadata needs to be made explicit, that is, captured and persistently linked to the record.

As capture of essential metadata is not typically built into the document creation and transmission process, the fault for failing to create records does not necessarily lie with the record creator/recipient. According to the [27]... even if one assumes the existence of a high level of motivation to ensure accountability, the very notion of what a record consists of is not as obvious as in the paper world, and the mechanisms for creating it may not be available to the potential record creator unless certain prior actions have been taken. To address challenges of metadata John McDonald [28]advocate for the need of implementing a front-end environment to ensure that documents could be captured with records metadata that reflected their source business processes [29] reported his attraction to an object-oriented environment that enforced business rules and captured business process metadata with records from the time of their creation.

Active Records Environment risk

Record-keeping systems are distinguished from information systems within organizations by the role they play in providing organizations 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 [30].

Literature reviewed indicates that major risks in the life of electronic records occur prior to their ingestion into a record-keeping system, or transfer into an archival control environment. During this phase the records are liable to be altered, to lose their original identity, or to be separated from metadata required to establish their authenticity. To address this challenge [31] argue that the records must be kept in a record-keeping system and that any organization that want to use electronic documentation as evidence in the future will need to satisfy the requirements of evidence in the normal course of conducting its business.

From the literature reviewed it has been difficult to do so in the computer-based communications environments which organizations have implemented in the past because applications software sold by third parties have not met these requirements. Information systems are generally designed to hold timely, non-redundant and easily manipulated information, while recordkeeping systems store time bound, inviolable and redundant records. Few, if any, in-house information managers have been able to devote the energy to rigorous definition of the distinct requirements for recordkeeping or, if they had, would be able to envision how to satisfy these throughout all systems. Without such explicit and testable specifications, computing application and electronic communications systems have failed to satisfy the requirements for recordkeeping and are, therefore, a growing liability to organizations even while they are contributing directly to day-to-day corporate effectiveness [32].

These threats may be related to systems administration, use, and ongoing metadata acquisition or loss. Systems administration threats are, not specific to electronic record-keeping environments, but they pose a fundamental challenge in a system whose entire purpose is to preserve the integrity and authenticity of the records it holds. These threats can be addressed through good systems management practices – backup and recovery, database integrity, sound metadata management, ongoing data conversion, etc. As Hedstrom[33] put it, trusted systems are defined as systems that can be relied on to follow certain rules at all times. Record-keeping systems are a type of trusted system where rules govern which documents are eligible for inclusion in the record-keeping system, who may place records in the system and retrieve records from it, what may be done to and with a record, how long records remain in the system, and how records are removed from it.

Archival Environment

A record is a specific piece of information produced or received in the initiation, conduct or completion of an institutional or individual activity. It comprises sufficient content, context and structure to provide evidence of that activity. It is not ephemeral: that is to say it contains information that is worthy of preservation in the short, medium or long term [34].When users generate a Business Acceptable Communication, consisting of content encapsulated by all the metadata necessary to ensure its integrity and longevity, the record should be split off from the application systems environment and sent to a separate recordkeeping system where it will be kept intact. This means that systems implementers need to construct “traps” in which they can capture the business transaction along with the metadata required for evidence. Most of this data, such as the time of the transaction, the identity of the sender and recipient, and the structural dependencies of the data, can be readily adduced from information available to the application and operating environment. The issue is how to generate, and capture, the metadata which identifies the

business transaction-type or task of which the record is evidence [35].

During ingestion into a record-keeping system, whether by transfer from a management environment [or at the time of capture, there is considerable risk that adequate metadata to document content, structure, and context might not be recorded and/or stored irrevocably with the record. The Pittsburgh Project asserted that business process metadata (documenting the broad functional context) and structural metadata (documenting systems dependencies) could be captured automatically from electronic applications environments at the time of record capture.

Indeed, there was every reason to prefer a more conservative option, which placed a record-keeper and "registry" function between the creation and ingestion, and made a traditional assignment of metadata through classification.

The theory based on the Pittsburgh Project always left this possibility open, as the italicized statement below makes clear. The functional requirements for evidence in recordkeeping dictate the creation of records that are comprehensive, identifiable (bounded), complete (containing content, structure and context), and authorized. These four properties are defined by the requirements in sufficient detail to permit us to specify what metadata items would need to describe them in order to audit these properties. This descriptive metadata cannot be separated from them or changed after the record has been created. Several additional requirements define how the data must be maintained and ultimately how it and other metadata can be used when the record is accessed in the future. The metadata created with the record must allow the record to be preserved over time and ensure that it will continue to be usable long after the individuals, computer systems and even information standards under which it was created have ceased to be. The metadata required to ensure that functional requirements are satisfied must be captured by the overall system through which business is conducted.

Unfortunately, this remains an area where there is much confusion about what needs to be controlled in order to ensure authentic records. The UK Functional Requirements for Electronic Records Management Systems which is widely used do not even provide for capture of database transactions; all issues relating to the authenticity of databases and actions with respect to them are completely neglected, meaning also that records received from such databases by users employing standard database access methods (e.g., querying a database that they have permission to view) are not being recorded at all. Yet the user has how the organization accomplished its functions and activities[36].

Preservation risks for electronic records

Perhaps the greatest risk to electronic records is preserving the records' authenticity over time. Currently in Kenya as elsewhere in the world there is no clear method to ensure that electronic records can be preserved over time. While it is a requirement that the records must remain under the control of the archival recordkeeping system at all times, the reality is that all the methods that are currently used for preserving electronic records require that software external to the archival recordkeeping system be employed , either to migrate data or to emulate operating systems. The transition to new formats or media signal a moment of risk. Migration of formats and emulation of systems depend on tests for accuracy and completeness that rely on human judgment, entirely outside the control of systems. Because preservation carries risk of loss of authenticity – through loss of metadata, changes in renditions, and, even, loss of content – there has been a growing agreement that the original bit-stream should simply be kept along with migrated formats as a kind of double insurance.

REFERENCES

1. Lowry, Thurston; Aligning Records Management with ICT/ e-Government and Freedom of Information in East Africa. International Records Management Trust, 2014.
2. Ibid.
3. IRMT; The E-records Readiness Tool. London: International Records Management Trust, 2004.
4. Wamukoya J, Mutula S; Transparency and Integrity in Government: Building Capacity for Managing Electronic Records in the Eastern and Southern Africa Region. 2005.
5. Akotia P; Financial Records Management Project: Phase Three Submitted to the Government of Uganda, 2000.
6. Kemoni HN; Records Management Practices and Service Delivery in Kenya.PhD Thesis; University Kwanzulu Natal. 2007.
7. IRMT; Managing records as Reliable Evidence for ICT/e-Government and Freedom of Information .Kenya Country Report, 2011.
8. Wamukoya and Mutula, 2005. See note 4.
9. Ibid. Wamukoya and Mutula, 2005.
10. Kemoni [see note 6]
11. IRMT 2011 [see note 7]
12. Kemoni[see note 6]
13. Wamukoya&Mutula[see note 4].
14. IRMT; 2003. A summary report on the IRMT/World Bank evidence –Based governance in the Electronic age global forum Electronic discussion on Information Technology, electronic

records at record keeping held between 27-31 January
15. IRMT, 2003 [see note 14].
16. Ibid.
17. Ibid.
18. MacNeil H; "Protecting Electronic Evidence: A Final Progress Report on a Research Study and Its Methodology."Archivi and computer, 1997; 7:1-2
19. Bearman D; Moments of Risk: Identifying Threats to Electronic Records E-Government Policy Framework for Electronic Records Management, 2011
20. InterPARES Strategy Task Force, 2000. http://www. interpares.org/ book/interpares _book_g_part4.pdf (Accessed 20 January 2016)
21. Pittsburgh Project, 1996; University of British Colombia, 1998; InterPARE 1&2.
22. Committee on Electronic Records; Guide for Managing Electronic Records from an Archival Perspective. 2010.
23. MacNeil, 1997 [see note 18]
24. The InterPARES Project, 2000. See note 20.
25. Bearman D; Item Level Control and Electronic Record Keeping .Archives and Museum Informatics, 2006;10(3):95-245
26. McKemmish S; Describing Records in Context in the Continuum: The Australian Record kepeeping Metadata Schema. Archivaria, 2002; 48:3-43.
27. ICA Committee on Electronic Records, "Guide for Managing Electronic Records.
28. John McDonald, 2006.
29. Thibodeau K; Building the future: The Electronic Records Archives Program. Bearman, 2003.
30. Bearman, 2011 [see note 19]
31. Ibid.
32. Ibid.
33. Hedstrom. 2006
34. Saffady W; Records and Information Management :Fundamentals of Professional Practice 2nd edition ARMA international overland Park, Kansas, 2011.
35. Bearman, 2011 [see note 19]
36. Ibid.