Trustworthiness of digital records in government accounting system to support the audit process in Botswana

Olefhile Mosweu
Department of Information and Knowledge Management, University of Johannesburg, Johannesburg, South Africa, and

Mpho Ngoepe
Department of Information Science, University of South Africa, Pretoria, South Africa

Received 8 November 2019
Revised 16 January 2020
6 August 2020
Accepted 21 December 2020

Abstract

Purpose – The purpose of this study is to explore how the trustworthiness of digital records generated in an enterprise resource planning (ERP) system known as the government accounting and budgeting system (GABS) is maintained to support the audit process in the public sector of Botswana.

Design/methodology/approach – This qualitative study used modern archival diplomatics as a theoretical framework to examine the procedures for authenticating digital accounting records in GABS to support the audit process in Botswana. Data were collected through interviews and documentary reviews.

Findings – The study established that although GABS is not a record-keeping system, it generates digital records. In the absence of procedures, auditors rely on social and technical indicators (system application controls) to authenticate records.

Research limitations/implications – The findings of the study are limited to the case study and cannot be generalised to other organisations.

Practical implications – The findings of the study can inform the necessary measures that can be taken to ensure that digital records generated in ERPs are maintained authentic to support financial auditing processes. In addition, the paper also presents differing approaches by records managers, auditors and information technology specialists to evaluate the authenticity of records in digital systems, thus contributing to the literature about professional allies and competitors to archivists and records managers.

Originality/value – This paper provides empirical evidence from an original study.

Keywords Public sector, Records management, Botswana, Auditing, Records, Accounting system

Paper type Research paper

1. Introduction

The deployment of computer systems to process financial and other data, and to perform, monitor and control their operational and administrative operations has become a norm as global developments took root over the need for improved financial management (Porter *et al.*, 2003). This resulted in the increased introduction of the Integrated Financial Management Information System (IFMIS) for purposes of promotion of efficiency, effectiveness,

The study was made possible by a Research Development Grant for InterPARES Team Africa Project by the National Research Foundation of South Africa. Grant number 105739.

0956-5698
DOI 10.1108/RMJ-11-2019-0069

accountability, transparency, the security of data management and comprehensive financial reporting (Hendricks, 2012). Simultaneously, many economies around the world, thus, transitioned from primarily paper-based administrative systems to digital systems through the application of information and communication technology (ICT) as part of e-government initiatives (Lemieux, 2015). The proliferation of ICTs in public sector organisations has been attributed to a number of reasons, including the need to account for the use of public resources and to improve the delivery of services (Heeks, 1998; Hendricks, 2012).

Conducting business processes in a digital environment has meant that digital records are generated. When it comes to accounting as a form of demonstrating accountability for the use of resources, including public monies, records remain a vital resource. Automation of auditing and accounting processes is done through the implementation of business systems. The International Council on Archives (ICA) (ICA, 2013) defines a business system as "an automated system that creates or manages data about an organisation's activities". A business system includes applications that facilitate transactions between an organisational unit and its customers. Specific examples include the e-commerce system, client-relationship management system, purpose-built or customised database or finance or human resources systems (ICA, 2013; Uniting Church in Australia, 2017). According to the ICA (2013), a business typically contains "dynamic data that is commonly subject to constant updates (timely), are able to be transformed (manipulable) and holds current data (non-redundant)". Kastenhofer (2016) observes that business systems create and keep great quantities of digital records.

As such, auditors have come to rely on computers as a tool for conducting auditing procedures (Porter *et al.*, 2003) and for them to make audit opinions, they need authentic records (Bhana, 2008; Ngoepe and Ngulube, 2014). Notably, a lot of business systems are not necessarily equipped with capabilities for the medium and long-term preservation of records (McLeod, 2012). The systems are originally meant to support business processes, and unless the business process requires the capture of those records in designated record-keeping systems, those records will most likely stay undeclared in their home environment (Johnston and Bowen, 2005; Charles Darwin University, 2014).

Without proper records of transactions, the objective of auditing, which is to ascertain the accuracy and reliability of financial statements and to possibly identify fraud, becomes difficult (Ngoepe, 2004). This is also the case in the digital environment. For example, Ngoepe and Ngulube (2013) observed that audit reports prepared by the Auditor-General of South Africa on an annual basis indicate that poor record-keeping partly contributed to disclaimed audit opinions in the public sector. In Zimbabwe, a study by David (2017) ascertained the contribution of records management to audit opinions and accountability in government entities and found that inadequate and inconsistent records management within government entities was associated with adverse and qualified opinions and, in some cases, unqualified opinions. On a general note, Okello-Obura (2012) reviewed the literature on records management as a conduit for effective auditing and noted that a lack of supporting records during the audit process is a sign of poor accountability and a lack of regulatory mechanisms in organisations. All these examples point to the fact that audit processes should not only be concerned with accounting for the use of funds but also with how records are managed. This includes digital records produced and stored in accounting information systems. Many times, these records are excluded from organisational record-keeping systems, which leads to difficulties in authenticating records created in such systems (Ngoepe, 2012). It is also notable that financial records systems have audit functionalities, which serve as good indicators of internal business controls, and tracks information integrity in the system. Such information can be confidential and sensitive information such as financial data. For keeping records in the financial system in the long

term, such systems can be integrated with an EDRMS. Thus, Ngoepe and Ngulube (2014) assert that there is a symbiotic relationship between records management and the entire accounting function because the accounting cycle begins with the creation of a record. Furthermore, Akotia (1996) is of the view that proper finance management would be possible in organisations when there is an adequate cross-reference between records management and accounting systems.

1.1 The use of information and communication technologies in the Botswana Government's accounting processes

The Government of Botswana's Ministry of Finance and Economic Development (MFED) implemented the GABS in 2004 for similar reasons. It is operational in most government offices across the country. The custodian of GABS is the AGD, within the MFED. According to the Office of the Auditor-General of Botswana (OAGB) (2008), GABS was implemented specifically to achieve the following:

- Increase the ability to undertake central control and monitoring of expenditure and receipts in the ministries and departments.
- Provide up to date and online information on the government's cash position, economic, financial and operational performance.
- Eliminate the duplication of maintaining the same information.
- Faster processing of budget preparation, closing of accounts and processing of other transactions.
- Enhance the ability to demonstrate accountability to donors and the public by having a proper audit trail of transactions in the system.

GABS, an ERP system, was developed using the modules of Oracle Financials such as general ledger, payables, receivables, public sector budgeting and cash management. In these processes, digital records are created. For business convenience, GABS has been divided into different functional modules being:

- Budget Administration Module.
- Main Accounting System.
- Revenue Office Data Module.
- Votes Ledger Module for Common Ministries.
- Public Debt Servicing Module.
- Agencies Module to cater for two fund accounts being the Mine Workers' Fund and the Guardian Fund.
- Cash Flow Module.

The different modules in GABS are used to perform different financial transactions and these create digital records. The systems are originally meant to support business processes, and unless the business process requires the capturing of those records in designated record-keeping systems, those records will most likely stay undeclared in their home environment (Johnston and Bowen, 2005; Charles Darwin University, 2014). Being a computerised information system, GABS generates digital accounting records. The system is described as a reasonably well-developed information system (DFC Consortium, 2013), a conclusion reached when the DFC Consortium undertook a Public Expenditure and Financial Accountability Assessment in Botswana.

1.2 Authenticating digital records

The transition from a paper environment to a digital environment in terms of conducting business processes meant that most of the information required for auditing is provided through a networked environment (Moorthy *et al.*, 2011). The digital environment provides challenges related to authenticating records produced by accounting information systems such as GABS. In the digital environment, records authenticity is a major threat as records are predisposed to be easily tampered with or corrupted, either accidentally or maliciously (Duranti, 2009:52). Authenticity is one of the four characteristics of a record, together with usability, integrity and reliability (International Standards Organisation, 2016). It refers to its trustworthiness and the fact that it has not been tampered with or corrupted, either accidentally or maliciously (Duranti, 2009). According to the National Archives of United Kingdom (2003), the authenticity of a record in a digital environment can only exist if adequate features of the other three characteristics are present. According to the National Archives and Records Administration (NARA) (2005), for records to remain reliable and authentic, with their integrity maintained and be useable for as long as they are needed, their content, context and sometimes structure have to be preserved. According to Rogers (2015), modern societies rely very much on records for various purposes; hence, records management professionals acknowledge and identify record's authenticity as necessary for their preservation. According to Ngoepe and Ngulube (2014), auditors need records as evidence of transactions not only to be available but also reliable as well. This is because they may be available, but they may also be incomplete and their authenticity may not be guaranteed.

Digital records generated in information systems, some of which do not have records management functionalities can be authenticated in a number of ways. These include reliance on technical and social indicators, digital signatures, policies and procedures and blockchain technology (Rogers, 2015; Stančić, Ngoepe and Mukwevho, 2019; NARA, 2005). According to Rogers (2015), deciding whether records are authentic is based on both technical and social indicators. To put this into perspective, Rogers (2015:112) puts forward the idea that "in the digital environment a presumption of authenticity is an inference based on evidence about how the records have been created and maintained". Compliance to policies and procedures amongst others depicted as social indicators gives assurance that the digital records in the system have maintained their authenticity, as creation, and therefore, can be regarded reliable. Table 1 presents the social and technical indicators used to establish the authenticity of a digital record.

As records in the digital environment can be easily forged or altered and that may be harder to detect compared to paper records, authenticating records to establish their authenticity is crucial (Uganda Law Commission, 2004). Establishing the authenticity of an archival document is reliant upon establishing and preserving the identity and the integrity of a record from its point of creation and thereafter (Lemieux, 2015). That is where technical indicators of records authenticity are applicable. Both Duranti and Preston (2008) and Duranti and Blanchette (2004) aver that the presumption of authenticity is based on the number of requirements that have been met and the degree to which each has been met such that the more requirements are met the more record is deemed authentic.

Blockchain technology provides an opportunity for ensuring that once records are created, their integrity can be maintained. Digital signatures that attest to the authenticity of records can be retained in a blockchain. Morabito (2017) shows that digital signatures and communication security(cryptography) are used to authenticate, verify user identity and implement access rights in a read or write format, bringing great difficulty in altering a record. NARA (2005) says that in that case these could be re-hashed to determine if any

Social indicators	Technical indicators
Written policies and procedures governing the management of the records system	Information about the software used to create and manage the digital records
Documentation about the record system (design, operation, management, etc.)	Information about changes made to the digital records over time, (e.g. migration, normalisation, etc.)
Written policies and procedures governing digital records	Information about actions taken to preserve the digital records
Classification scheme and/or file plan	Access controls/security measures
Retention and disposition schedules	Audit logs
Archival description	Cryptographic validation techniques (e.g. digital signatures, hash digests, etc.)
	Standardised metadata

Source: Rogers (2015, p. 113)

Table 1. Indicators of authenticity

changes or alterations have been made after creation. To achieve this, blockchain uses cryptographic signatures and public keys to form a chain-linked record of transactions, which cannot be forged (NARA, 2005).

Determining the authenticity of digital documents for purposes of auditing is problematic (Park, 2001; Barrister, 2006). In South Africa, for example, Mulaudzi *et al.* (2015) note that auditors have rejected digital records as evidence during audits because their authenticity was questionable. This is because the criteria used by auditors to judge the authenticity of digital records for them to support the audit process are not clear (AGSA, 2014:68).

In the context of Botswana, where a public sector organisation submits digital records as evidence to support the audit process, both the auditee and the auditor need to ensure that the audited records are authentic and reliable (Mosweu, 2011; Mosweu, 2018). The records need to be assessed, analysed or investigated for their authenticity.

A study of financial records and information systems in the AGD in Botswana by the International Records Management Trust (IRMT) (2004) revealed a lack of records management policies and procedures to guide the management of digital accounting records in GABS. Consequently, IRMT (2004) recommended that a records management policy and procedures be developed in collaboration with the Department of Botswana National Archives and Records Services (BNARS). If the policy and procedures are in place, it would ensure an integrated approach to creating, maintaining, accessing, preserving and disposing of both paper and digital records in the system. IRMT (2004) adds that the policy should cover the legislative and regulatory requirements relating to financial records management, the definition of records and their key characteristics (such as evidentiary quality, authenticity and reliability), the purpose of records (accountability and audit), requirements for record-keeping and system design (paper and electronic), standards for financial records management, skills and competencies for managing records and user responsibilities.

1.3 Archival diplomatics and digital records authenticity

This study was guided by concepts from Archival diplomatics. The concepts come from principles derived from archival science and diplomatics. As far back as the late 17th century Europe, the need to maintain records authenticity and indirectly records reliability, was a contemporary issue then, for purposes of establishing the existence of patrimonial

rights of the church, religious orders and other authorities. This helped to identify and eliminate forgeries (Duranti, 1997; Jantz, 2009). Diplomatics concerns itself with establishing the authenticity of archival documents as single entities. It identifies those features of documents that make them records i.e. fixity, reliability, completeness and representations of transactions. Over time such features are crucial in records perseveration as preserving a record requires preserving all those features that make it a record (Roeder *et al.*, 2008).

Archival science complements diplomatics very well in relation to the question of records authenticity, though it looks at records as aggregates, not single items. Records authenticity is a fundamental aspect in Archival Science. In archival theory, records that are relied upon by the creator to transact organisational business are presumed authentic (Duranti and Blanchette, 2004). Furthermore, for Jenkinson (1937), archival documents were authenticated by merely being preserved in archival custody. Cook (1986) disputed this view, preferring instead that records first be tested for indications of their authenticity through studying their provenance and elements of their form (diplomatics).

Digital technology has altered the creation of reliable records and the means of presuming their authenticity over time and across the technological change. Unlike paper records, they are volatile and subject to lose, intentional or unintentional alteration, contamination or corruption, even when they are still in the custody of their creator (Gilliland-Swetland, 2005). It is difficult to determine their authorship, provenance and chain of custody due to the easiness of being copied, shared and transmitted. According to Rogers (2016:17):

> "Even if the creator relies on a digital record in the course of business, and maintains its unbroken chain of custody, the fragility and vulnerability of digital records demands explicit action to protect the record's authenticity".

The InterPARES (2002) requirements for assessing and maintaining the authenticity of electronic records framework was used to assess the authenticity, and thus the trustworthiness of digital records generated and stored in GABS. In modern archival diplomatics, this entailed assessing components of a record generated in the system by specifically assessing the metadata of the records as linked to the records by provenance, administrative procedure and form, as well as legitimate custody, as well as system operational and technological mechanisms (MacNeil, 2000; Duranti *et al.*, 2002; Rajh, 2016). Establishing methods of authenticating records generated and stored in GABS was the purpose of this study. This was in view of the fact that systems are still designed to manage data rather than records and that although some systems contain entities satisfying the diplomatic definition of a record, they do not retain enough information about their identity and integrity (Roeder *et al.*, 2008).

That said, it is clear that the maintenance of records authenticity is different theoretically and in practice when dealing with both paper and digital records. This study used modern archival diplomatics as a theoretical lens in the endeavour to guide the resolution of the research question which was to examine the procedures for authenticating digital accounting records in GABS to support the audit process in Botswana.

2. Problem statement

The authentication of digital accounting records created and stored in the GABS of the Botswana Government, particularly for purposes of their acceptance in the audit process, is yet to be determined. This is in spite of the fact that audit opinions are offered on the basis of available, accurate and complete records. According to IRMT (2004), there was a lack of documented procedures to authenticate records in the system. The Office of the

Auditor-General of Botswana has been unable to use records in the audit process because they were deemed not authentic enough to support the audit process (OAGB, 2008; Mosweu, 2011; Pinielo, 2015). Specifically, records were found to be unauthentic to support the audit process at the Gaborone City Council, Kgatleng Land Board, Public Procurement and Disposal Board, Ministry of Trade and Industry, the Independent Electoral Commission and Air Botswana. The Auditor-General lamented that records consulted were incomplete, misplaced, misfiled, haphazardly stored, difficult to retrieve, poorly classified and fragmented.

The rejection of digital records in the audit process because of their questionable authenticity has also been reported in the South African public sector because they could not be used to support audit queries (Mulaudzi *et al.*, 2015). The nature of digital records is that proving their authenticity is difficult over and above the fact that the criteria used by auditors to declare records authenticity are unclear (Park, 2001; Barrister, 2006; AGSA, 2014). It is easy to alter and manipulate digital records without leaving any trace (International Auditing and Assurance Board, 2010). Rogers (2015) opines that procedures and policies can be used to authenticate digital records socially while, technically, they can be authenticated through the use of IT system application and general controls. Using archival diplomatics as a theoretical lens, this study reports on procedures for authenticating digital accounting records in GABS to support the audit process in Botswana's public sector.

2.1 Research question

The main purpose of the study was to explore how the trustworthiness of digital records in the government accounting system is ensured to support the audit process in Botswana. The following sub-questions were used to explore the main theme:

- What procedures are in place to support the creation and maintenance of authentic digital records?
- What functionalities does GABS have to ensure that it creates and maintains authentic reliable digital accounting records?
- What criteria are used to declare records authentic?
- Has the authenticity of accounting records in GABS ever been in question during audits and rejected as evidence in the audit process?

3. Research methodology

This study focused on financial auditing which is undertaken by the Office of the Auditor General of Botswana. It was limited to the Accountant General's Department as the principal study location. Other government departments were excluded largely because the AGD is the custodian of GABS and coordinates its implementation across the whole of the central government. Local government departments were also excluded as they do not use GABS in their accounting functions. Located within the interpretive research philosophy (Jupp, 2006; Thanh and Le Thanh, 2015), this study used the qualitative research approach (Creswell, 2014) in its endeavour to investigate the procedures in place to authenticate digital accounting records transacted through GABS to support the audit process in the public sector of Botswana. This paper reports on the findings of a doctoral study in which the first author was the principal investigator while the second author was the supervisor. Qualitative studies are conducted in natural settings with subjective meanings constructed

from an understanding emanating from the minds of participants (Leedy and Ormrod, 2005). The interview method was used as the data collection tool.

The population for this study was made up of all central government ministries and departments. Ngulube (2005) advises that a study population needs to be well defined prior to data collection, as an appropriate sample size will reflect the population as precisely as possible. The population for this study was made up of 25 mainline ministries of the Government of Botswana and six quasi-government departments. The system under study, GABS, has been implemented in all government ministries and departments, including the quasi-government departments. From the study population, as derived from the Botswana Telecommunications Corporation's telephone directory (Botswana Telecommunications Corporation, 2017), six were purposively selected to take part in the study on the basis of their function in the public sector of Botswana.

- Botswana National Archives and Records Services: mandated to manage public sector records across their life cycle, regardless of media or format.
- Department of the Accountant General: responsible for the compilation and management of government accounts, custody and safety of public money and its disbursement, through GABS.
- Department of Information Technology: coordinates computerisation of government projects.
- Office of the Auditor General of Botswana: audits government ministries and departments, including financial or regularity audits.
- Department of Corporate Services in the Ministry of Finance and Economic Development: responsible for the coordination of support services for the entire ministry, including records management.
- Department of Internal Audit within the MFED: provides internal audit services within MFED (including an audit of GABS), as well as for the entire government through internal auditors seconded to government ministries and departments.

The study participants were selected purposively and these included auditors from the OAGB and the Department of Internal Audit records managers and accountants from the Ministry of Finance and Economic Development and records managers from the Botswana National Archives and Records Services. ICT personnel from the Department of Information Technology and AGD also took part. A total of 25 participants took part in the study and were interviewed through email communication. The researchers had planned to be tape-recorded in a face to face interview scenario but they refused and preferred not to have responses captured on tape. They felt comfortable and nervous. In addition, during the period of data collection, the system (GABS) was being upgraded and so the participants were attending a series of consultative workshops that were generally available for face-to-face interviews which can be lengthy. The participants were, however willing to take part in further email communications and follow-up telephone calls. The interview questions were developed from the literature consulted. The questions are presented at the end of the paper as Appendix, inclusive of Table 2. To maintain the privacy and confidentiality of study participants, they were coded. The responses were summarised into themes as guided by research questions. Records managers were coded as RM1 up to RM7, ICT professionals were coded as ICT1, ICT2 and ICT3, while auditors were coded as IA1 up to IA4 (internal auditors) and AG1 to AG5 (external auditors). System analysis supplemented the data collected through interviews. It concentrated on the components of a record as theorised by archival diplomatics. System analysis studies the constituent parts of an information system

Benchmark requirement for assessing records authenticity	Yes	No
Access privileges: the creator has defined and effectively implemented access privileges concerning the creation, modification, annotation, relocation and destruction of records		
Protective procedures: loss and corruption of records: the creator has established and effectively implemented procedures to prevent, discover and correct loss or corruption of records		
Protective procedures: media and technology: the creator has established and effectively implemented procedures to guarantee the continuing identity and integrity of records against media deterioration and across the technological change		
Establishment of documentary forms: the creator has established the documentary forms of records associated with each procedure either according to the requirements of the juridical system or those of the creator		
Authentication of records: if authentication is required by the juridical system or the needs of the organisation, the creator has established specific rules regarding which records must be authenticated, by whom and the means of authentication		
Identification of authoritative record: if multiple copies of the same record exist, the creator has established procedures that identify which record is authoritative		
Removal and transfer of relevant documentation: if there is a transition of records from active status to semi-active and inactive status, which involves the removal of records from the electronic system, the creator has established and effectively implemented procedures determining what documentation has to be removed and transferred to the preserver along with the records		

Source: InterPARES (2002)

Table 2. Benchmark requirement for assessing records authenticity

to identify its objectives (Tutorials Point, 2015). Through the analysis, the requirements for an information system to support organisational activities are identified and documented (Livari *et al.*, 2006). The main interest was to assess whether GABS possessed all the necessary metadata elements that enable an information system to generate and maintain authentic records that can be trusted for the audit process because they are trustworthy.

4. Research findings and discussion

This section analyses and presents the results of the data obtained via interviews. This study revealed that participants possessed diverse educational qualifications ranging from archives and records management, computer information systems, accounting and finance, business studies, strategic management to computer science. The qualifications are appropriate for archives and records management professionals, ICT specialists and auditors. In terms of the work experience of the study participants, their work experience ranged from two years to more than 27 years. This suggests that they have some experience in their professional field. The presented study findings are limited to procedures in place to maintain the authenticity of digital accounting records created and stored in GABS.

4.1 Procedures to support the creation and maintenance of authentic digital records

This question was posed to records management professionals at both BNARS and the Department of Corporate Services (DCS) at MFED. BNARS is mandated by the National Archives and Records Services Act to coordinate the management of Botswana public sector records, including digital records (Ngoepe and Keakopa, 2011; Mosweu and Ngoepe, 2018; Mosweu, 2019). Records managers are responsible for the management of records

across the entire MFED. The AGD does not have a records manager. The following were the responses:

> *RM2*: *Not yet. The government is still in the process, through the e-government cluster, to provide a policy framework and guidance for electronic records management, which will be applicable in all government offices.*
>
> *RM3*: *None that I am aware of.*
>
> *RM4*: *There are no procedures in place.*
>
> *RM5*: *BNARS currently is more focused on the management of physical records, as they are the most created by ministries and departments. This means that as system-generated records are printed, BNARS may consider storing such records in its repositories/records centres. So, there are no procedures for digital records.*
>
> *RM6*: *It has not developed procedures specifically for digital records, but the National Archives and Records Services Act and the Records Management Procedures Manual cater for all records.*
>
> *RM7*: *Nothing has been developed yet, rather there is so much dependence on the acts and policies and BNARS procedures.*

It is clear from the findings that there is not much on the ground in terms of available guidance regarding procedures for the maintenance of authentic records in digital systems provided by BNARS, as expected. There is no national records management policy or procedures to guide the maintenance of digital records authenticity although there are many implemented e-government systems, which generate digital records when services are rendered to citizens. ISO 15489–1 (2016) also advocates for the implementation of records policies that promote the creation of records that possess records management characteristics which include records authenticity and integrity. A number of studies have also found that there is a lack of infrastructure and guidance for the management of digital records in Botswana (Moloi, 2009; Ngoepe and Keakopa, 2011; Ngoepe and Saurombe, 2016). This state of affairs is common across the ESARBICA region with South Africa as an exception (Kemoni, 2009; Keakopa, 2010; Nkala *et al.*, 2012).

4.2 Government accounting and budgeting system functionalities for ensuring the creation and maintenance of authentic digital accounting records

Auditors rely on authentic records in the audit process as such records serve as evidentiary documents (Dandago, 2009). To express audit opinions, auditors need a sufficient supporting audience (InterPARES, 2018). Lack of such evidence points to poor accountability and governance in an organisation, which can lead to disclaimer opinions and increased costs of auditing (Ngoepe, 2012). The question above was directed to ICT professionals based at the Department of Information Technology (DIT), which coordinates government ICT-based system implementation. ICT professionals gave the following answers to the posed question:

> *ICT1*: *There are security controls that are implemented in the GABS. The segregation of duties enables the integrity of the record in the system. There is a validation of records before they are authorised.*

ICT2: Computer security mechanisms are inbuilt in the system to ensure that records created and maintained in the system retain their integrity. For example, access to the system is controlled by using passwords. The creation of records is centralised, e.g. to create a company profile, authority is sought from the ministry and personal data is extracted from the HCM Oracle system. The creation of records is centralised, e.g. to create a company profile, authority is sought from the MFDP and personal data is extracted from the HCM Oracle system.

ICT3: -Usernames and passwords are created for anyone using GABS.

-Username is linked to the employee and user department.

-Responsibilities/functions are created according to a department and assigned to officers in that department only.

-Security rules are created so that offices who are given access to transact in the system are only able to consume/spend only funds allocated to their department.

-The officer creating a transaction cannot validate/authorise it.

-The system does not allow a paying officer to pay a supplier with the same invoice number more than once.

-All transactions created and validated cannot be deleted, they are rather cancelled to keep an audit trail.

-All transactions since implementation are available in the system and can be retrieved as and when required based on the parameters, e.g. transactions by period, by department or even by the supplier.

-The system can only be accessed by those in the government data network.

The findings revealed that GABS relies heavily on IT system general and application controls for ensuring that records created in the system are maintained authentically. These are the very metadata elements some of which are stated in the requirements for assessing and maintaining the authenticity of records generated in digital systems as theorised by archival diplomatics (InterPARES, 2002). This is not surprising, as GABS, being an ERP, is not a record-keeping system. Records authenticity is a fundamental concept in archival science and has a theoretical foundation (Rogers, 2016). For ICT professionals, the authenticity of digital records in GABS is ensured through the following:

- Segregation of duties.
- Inbuilt computer security mechanisms.
- User names and passwords.
- Audit trails.
- People outside the government cannot access GABS.
- Records in the system cannot be deleted, only cancelled.

A system analysis of GABS also show that it met all the requirements for assessing records authenticity, which are the following:

- Access privileges.
- Protective procedures: loss and corruption of records.
- Protective procedures: loss and corruption of records.
- Establishment of documentary forms.
- Authentication of records.
- Identification of authoritative record.
- Removal and transfer of relevant documentation.

From the analysis, thus in terms of modern archival diplomatics, the system generates records that qualify to be recorded. Furthermore, the metadata elements required to support records authenticity are available through the system. For ICT professionals, much reliance is placed on the use of equipment to maintain the authenticity of records. Rogers (2015) attests that indicators of records' authenticity can be social and technical. The technical indicators result from work processes or state changes in the records (as represented by system metadata capturing date created and date modified). They are system generated or implemented by the technological components of the overall records system. According to Rogers (2015), technical indicators focus more on controlling the system in which records reside. By controlling the environment in which records reside, their authenticity can be ensured. Locally, in a study that investigated the use of a Court Records Management System (CRMS) for the delivery of justice in the Gaborone Magistrate district in Botswana, information technology and system controls were used to protect the authenticity of records in the system (Mosweu and Kenosi, 2018). The British Broadcasting Corporation (2010) also prescribes through its Records Management Standard that it should be possible to provide adequate protection of the integrity of records for auditing purposes.

4.3 The criteria used to authenticate digital accounting records by auditors

When auditors undertake an audit assignment of financial records produced by business systems, they may ask a number of questions to determine whether the audit evidence can be reliable and authentic (Illinois Department of Revenue, 1998). These may include, "Are digital records available"? "What controls are in place to safeguard the records"? "Are the digital records reliable"? "Do the internal controls produce an acceptable level of assurance that the records are reliable"? "Do undocumented system changes exist"? "Is there an audit trail"? These are not all the questions they may ask but are merely an extract of possible questions. Answers to these questions facilitate the audit engagement. Notably, auditors have rejected digital records as evidence during audits because their authenticity was questionable (Mulaudzi *et al.*, 2015). This is because the criteria used by auditors to judge the authenticity of digital records for them to support the audit process are not clear (AGSA, 2014). Auditors were asked about the criteria they used to declare records as authentic, and thus acceptable in the audit process. The following were their responses:

> *IA1*: *We have a tool called Audit Command Language (ACL) which we use to check the integrity of data maintained by GABS. It is a governance risk and compliance tool. There are functions and commands that we run to verify data depending on the scope, objectives and tests of our audit assignment. The tests can be analytical or substantive. Therefore, we would accept that all fields that we require should have been completed with correct information. Where there are exceptions, it will be an indication that the integrity of data could have been compromised and, therefore, cannot be relied on. If data is compromised, audit decisions can be negatively affected and the audit may not go on.*

IA2: *Through data integrity. Auditors use a data analytical tool (ALC) to check the authenticity of data.*

IA3: *Auditors have a validation process of data prior to starting audit work. Data tests that can be done include formatting of data, checking for data completeness, data verification, checking for gaps, totals controls and others.*

IA4: *Audit trails and tests of data completeness. These tests are analytical procedures as they rely on the use of analytical tools to run tests such as IsBlank. The tests can be tests of data formats and blank fields of required or mandatory fields.*

AG1: *Data extraction is done in the presence of auditors. Integrity checks are performed first through a walkthrough to validate the controls in place. Data analysis is done to check if the data conforms to the business rules. Extraction is done either through in-built application reports or using SQL scripts to get the data we need.*

AG5: *There are some tools used to check if the records are genuine. Data analysis tools such as the Interactive Data Extraction and Analysis (IDEA) are used. It is used for analysing data, checking duplicates and completing data.*

The findings show that auditors rely on IT-enabled controls and checks for ensuring that records in GABS remain authentic. They specifically use software such as ACL (internal auditors) and IDEA (external auditors) for checking the authenticity of records in the audit process. The benefits of computerised auditing are undeniable (Kanellou and Spathis, 2009; ACCA, 2011; Moorthy *et al.*, 2011; Rezaei, 2013). GAS is used by auditors to analyse and audit live data in a wide range of applications. It can also perform the same function from data that has been extracted from a system (Debreceny *et al.*, 2005). GAS can browse, analyse, sort, summarise, stratify, sample and apply calculations, conversions and other operations to audit a full set of accounting data (Ahmi and Kent, 2013). Determining the authenticity of digital documents for purposes of auditing is problematic (Park, 2001; Barrister, 2006). In South Africa, for example, Mulaudzi *et al.* (2015) note that auditors have rejected digital records as evidence during audits because their authenticity was questionable.

4.4 The audit process and questionable authenticity of records in government accounting and budgeting system

Without authentic and reliable records of financial statements, accounting officers would be unable to furnish the public audit oversight mechanism with documentation supporting the audit process (Ngoepe, 2004). Poor recordkeeping has been known to frustrate audit assignments and this has contributed to disclaimed audit opinions in the public sector (Ngoepe and Ngulube, 2013). In Zimbabwe, a study by David (2017) linked the contribution of records management to audit opinions and accountability in government entities. The study also found that inadequate and inconsistent records management within government entities was associated with adverse and qualified opinions and, in some cases, unqualified opinions. On a general note, apart from that, Okello-Obura (2012) reviewed the literature on records management as a conduit for effective auditing and noted that a lack of supporting records during the audit process is a sign of poor accountability and a lack of regulatory mechanisms in organisations. Study participants were asked whether the authenticity of records in GABS has been in question during audits, resulting in the audit evidence rejected. They responded as follows:

IA1: *Yes. The audit of payroll and human resource management indicated that data is not completely clean. When data in the system is compromised, the audit cannot go on as the data will not be fit for purpose. Such data is unreliable and cannot be used in an audit.*

IA2:Yes, during auditing of payroll and HR. There were inconsistencies in the data captured. The mismatch in data was identified and relevant officers worked on correcting the mismatch. It is not a one-day issue since it involved other stakeholders like government ministries and departments, especially those who capture or process transactions at those ministries and departments.

IA3: *Yes, there was a time payroll data showed double payments, but the payslips showed differently. The records could not be used.*

AG1: *Yes. There are cases where some parts of transactions are done offline such as requisitions. Authenticity checks are part of the data analysis. We collect it and perform several tests, and if there are issues that we identify, we communicate with the user ministries to give us evidence to check if the records (sampled) were accurate and, depending on the outcome, we reported on the results. Incomplete records cannot be used as audit evidence.*

AG2: *Yes, the schedule and the account (rate) are not in agreement.*

AG3: *Yes. One employee from one ministry was able to make fake payments using GABS. The figures did not match when compared to hard copies prepared manually.*

It is clear that auditors need accurate and authentic records in the audit process. In South Africa, many records managers have lamented auditors who do not always accept digital records as evidence to support the audit queries due to a lack of guidelines (InterPARES, 2018). Evidently, with some records of questionable authenticity in GABS, they could not be used in the audit process and were, thus, rejected. Similarly, Mulaudzi *et al.* (2015:2) note that auditors in the South African public sector have rejected digital records as evidence during audits because their authenticity was in question and could not be tendered as evidence in the audit process. According to Park (2001), authentic records are genuine. They are trusted as evidence in the audit process. The problematic nature of digital records such as that they are easy to be tampered with or corrupted either by accident or through deliberate means (Duranti, 2009), makes auditing in a digital environment a complex undertaking (Park, 2001; Barrister, 2006).

5. Conclusion and recommendations

The need to have procedures in place to authenticate digital records is not in doubt lest they be altered and/or manipulated by those with motivational reasons. If that were to happen, such records would not be accepted by auditors who audit records in GABS in the audit process. It has emerged from the findings that records management practitioners, auditors and ICT professionals use different methods to authenticate digital records created and stored in the system. Notably, ICT professionals rely on IT general and system application controls as do auditors. Additionally, the auditors also rely on auditing software to determine the authenticity of records in the system. For records managers, there are no procedures or policies on the management of digital records. The absence of policies to guide the management of digital records has also been reported by other studies conducted in the ESARBICA region, including Botswana (Moloi, 2009; Ngoepe and Saurombe, 2016). The conclusion reached by this study is that digital records in GABS are authenticated through the use of technical indicators, which focus more on controlling the system in which records reside (Rogers, 2015). That said,

GABS should be integrated with BNARS' NARMS to protect the authenticity of records in the system. As a government entity entrusted with the management of the public sector in Botswana, it is recommended that BNARS should lead the development and implementation of guidelines for ensuring the maintenance of digital records in GABS. It has been shown in this study that GABS has been integrated with other business systems and can be interfaced with dedicated record-keeping systems. Therefore, a study that focuses on an investigation of the requirements for integrating business systems into record-keeping systems with a focus on how such integration may impact the authenticity of digital records in the system is worth pursuing.

References

ACCA (2011), "Specific aspects of auditing in a computer-based environment", available at: www.chinaacc.com/upload/html/2013/06/27/lixingcundac36fcea5144f4d905d7ebace1f1e5a.pdf

Ahmi, A. and Kent, S. (2013), "The utilisation of generalized audit software (GAS) by external auditors", *Managerial Auditing Journal*, Vol. 28 No. 2, pp. 88-113.

Akotia, P. (1996), "The management of public sector financial records: the implications for good government", available at: www.msu.ac.zw/elearning/material/1174370018Pino%20Akotia%201996%20on%20governance.pdf

Auditor General of South Africa (2014), "Consolidated general report on local government audit outcomes, 2013-2014", available at: http://intranet/AGSADocuments/AuditReports/Documents/2013-14%20MFMA/MFMA%20201314%20Consolidated%20GR%20Part%207%20Section%204%20Status%20of%20performance%20management.pdf

Barrister, M.S. (2006), "Proof of the authenticity of a document in electronic format introduced as evidence", available at: www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/Proof_of_authenticity_of_a_document.pdf

Bhana, P. (2008), "The contribution of proper record-keeping towards auditing and risk mitigation: Auditor-General of South Africa's perspective", available at: www.khunkhwane.co.za/uploads/The%20Contribution%20of%20Proper%20Records%20Keeping%20towards%20auditing%20and%20risk%20mitigation%20%20Auditor%20General%20Perspective.pdf

Botswana Telecommunications Corporation (2017), *Phone Book 2017*, Botswana Telecommunications Corporation, Gaborone.

British Broadcasting Corporation (2010), "Records management standards for BBC", available at: www.bbc.co.uk/guidelines/dq/pdf/media/records_management_standards_v1.3.pdf

Charles Darwin University (2014), "Records management – capturing university records procedures", available at: www.cdu.edu.au/governance/doclibrary/pro-061.pdf

Cook, M. (1986), *The Management of Information from Archives*, Gower, Aldershot, Hants, England; Brookfield, VT, USA.

Creswell, J.W. (2014), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Los Angeles.

Dandago, K.L. (2009), *Advanced Accounting Theory and Practice*, Adonis & Abbey, London.

David, R. (2017), "Contribution of records management to audit opinions and accountability in government", *South African Journal of Information Management*, Vol. 19 No. 1, pp. 1-14.

Debreceny, R., Lee, S., Neo, W. and Toh, J.S. (2005), "Employing generalized audit software in the financial services sector: challenges and opportunities", *Managerial Auditing Journal*, Vol. 20 No. 6, pp. 605-619.

DFC Consortium (2013), "Public expenditure and financial accountability assessment", available at: www.academia.edu/31072426/Republic_of_Botswana_Public_Expenditure_and_Financial_Accountability_Assessment_Final_Report

Duranti, L. (1997), "The archival bond", *Archives and Museum Informatics*, Vol. 11 Nos 3/4, pp. 213-218.

Duranti, L. (2009), "From digital diplomatics to digital records forensics", *Archivaria: Journal of the Association of Canadian Archivists*, Vol. 68, pp. 39-66.

Duranti, L., Eastwood, T. and MacNeil, H. (2002), *Preservation of the Integrity of Electronic Records*, Kluwer Academic Publishers, Dordrecht.

Duranti, L. and Preston, R. (2008), "International research on permanent authentic records in electronic systems (InterPARES) 2: Experiential, interactive and dynamic records", available at: www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf

Duranti, L. and Blanchette, J.F. (2004), "The authenticity of electronic records: the InterPARES approach", available at: www.interpares.org/ip2/display_file.cfm?doc=ip2_book_complete.pdf

Gilliland-Swetland, A. (2005), "Authenticity task force report", in Duranti, L. (Ed.), *The Long-Term Preservation of Authentic Electronic Records: Finding of the InterPARES Project*, Archilab, San Miniato.

Heeks, R. (1998), "Information systems for public sector management working paper series paper no. 1 information systems and public sector accountability", available at: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014657.pdf

Hendricks, C.J. (2012), "Integrated financial management information systems: guidelines for effective implementation by the public sector of South Africa", *South African Journal of Information Management*, Vol. 14 No. 1, pp. 1-9.

ICA (2013), "Principles and functional requirements for records in electronic office environments recordkeeping requirements for database based business systems", available at: www.ica.org/sites/default/files/9.%20Recordkeeping%20Requirements%20for%20Database%20Based%20Business%20Systems.pdf

Illinois Department of Revenue (1998), "Electronic records and computer-assisted auditing", available at: www.mtc.gov/uploadedFiles/Multistate_Tax_Commission/Audit_Program/Resource/Pub-107.pdf

International Auditing and Assurance Board (2010), "International standard on auditing 500: audit evidence", available at: www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf

International Records Management Trust (IRMT) (2014), "Evidence-Based governance in the electronic age", available at: www.irmt.org/documents/research_reports/project_reports/Final%20DGF%20Report%20Revised.pdf

International Standards Organisation (2016), ISO 15489-1: Information and Documentation – Records Management, ISO, Geneva.

InterPARES (2002), "Requirements for assessing and maintaining the authenticity of electronic records", available at: http://interpares.org/book/interpares_book_k_app02.pdf

InterPARES (2018), "Ensuring authenticity and reliability of digital records to support the audit process (AF06)", available at: https://interparestrust.org/assets/public/dissemination/AF06-FinalReport.pdf

Jantz, R. (2009), "An institutional framework for creating authentic digital objects", available at: www.ijdc.net/index.php/ijdc/article/viewFile/103/86

Jenkinson, H.A. (1937), *Manual of Archive Administration*, New and Revised, Percy Lund, Humphries and Co., London.

Johnston, J.P. and Bowen, D.V. (2005), "The benefits of electronic records management systems: a general review of published and unpublished cases", *Records Management Journal*, Vol. 15 No. 3, pp. 131-140.

Jupp, V. (2006), "The sage dictionary of social research methods", Sage Publications, London.

Kanellou, A. and Spathis, C. (2009), "ERP systems and auditing: a review", available at: www.researchgate.net/publication/274076878_ERP_Systems_and_Auditing_a_Review

Kastenhofer, J. (2016), "Identifying digital records in business systems: the definition of a problem", *Journal of the South African Society of Archivists*, Vol. 49, pp. 1-13.

Keakopa, S.M. (2010), "Overview of archival and records management developments in the ESARBICA region", *Archives and Manuscripts*, Vol. 38 No. 1, pp. 51-77.

Kemoni, H.N. (2009), "Management of electronic records – review of empirical studies from the Eastern, Southern Africa regional branch of the international council on archives (ESARBICA) region", *Records Management Journal*, Vol. 9 No. 3, pp. 190-203.

Leedy, P.D. and Ormrod, J.E. (2005), *Practical Research: Planning and Design*, Pearson Prentice, New Jersey.

Lemieux, V.L. (2015), "One step forward, two steps backward? Does e-government make governments in developing countries more transparent and accountable?", available at: https://openknowledge.worldbank.org/bitstream/handle/10986/22496/One0step0forwa0ent0and0accountable0.pdf?sequence=1&isAllowed=y

Livari, J., Parsons, J. and Wand, Y. (2006), "Research in information systems analysis and design: introduction to the special issue", available at: https://pdfs.semanticscholar.org/112b/1cfef3687c56d9855481f2d21dd5b59ba590.pdf

McLeod, J. (2012), "On being part of the solution, not the problem: taking a proportionate approach to managing records", *Records Management Journal*, Vol. 22 No. 3, pp. 186-197.

MacNeil, H. (2000), *Trusting Records: legal, Historical, and Diplomatic Perspectives*, Kluwer Academic Publishers, Dordrecht.

Moloi, J. (2009), "E-records readiness in the public sector in Botswana", *ESARBICA Journal*, Vol. 28, pp. 105-127.

Moorthy, M., Seetharaman, A., Mohamed, Z., Gopalan, M. and San, L.H. (2011), "The impact of information technology on internal auditing", *African Journal of Business Management*, Vol. 5 No. 9, pp. 3523-3539.

Morabito, V. (2017), *Business Innovation through Blockchain*, Springer International Publishing, Milan.

Mosweu, O. (2011), "Performance audit in the Botswana public service and arising records management issues", *Journal of the South African Society of Archivists*, Vol. 44, pp. 107-115.

Mosweu, O. (2019), "Knowledge and skills requirements for a records manager in Botswana in the networked environment", *Journal of the South African Society of Archivists*, Vol. 52, pp. 110-132.

Mosweu, T. and Kenosi, L. (2018), "Implementation of the court records management system in the delivery of justice at the gaborone magisterial district, Botswana", *Records Management Journal*, Vol. 28 No. 3, pp. 234-251.

Mosweu, O. and Ngoepe, M. (2018), "Legal framework for auditing public sector accounting records in the digital environment in Botswana", in Ngoepe, M. and Fombad, M. (Eds), *Proceedings of the 9th ProLISSA Conference*, Cambridge Scholars Publishing, Newcastle, pp. 153-165.

Mosweu, O. (2018), "A framework to authenticate records in a government accounting system in Botswana to support the auditing process", PhD Thesis, University of South Africa, Pretoria.

Mulaudzi, M., Mukwevho, J. and Ngoepe, M. (2015), "Ensuring authenticity and reliability of electronic records to support the audit process", available at: https://interparestrust.org/docs/file/AF06_20160321_AuthenticReliableAuditAGSA_Proposal_Final.pdf

NARA (2005), "Records integrity and authenticity", available at: www.nap.edu/read/11332/chapter/7

National Archives of United Kingdom (2003), "Generic requirements for sustaining electronic information over time: 1 – defining the characteristics for authentic records", available at: http://webarchive.nationalarchives.gov.uk/20100604215648/https:/www.nationalarchives.gov.uk/documents/generic_reqs1.pdf

Ngoepe, M. (2004), "Accountability, transparency and good governance: the national archives and records service of South Africa's role in helping government to better service delivery to the South Africans", Proceedings of 7th annual conference, Polokwane, Vol. 7, pp. 1-18.

Ngoepe, M. and Keakopa, S.M. (2011), "An assessment of the state of national archival and records systems in the ESARBICA region", *Records Management Journal*, Vol. 21 No. 2, pp. 145-160.

Ngoepe, M. and Ngulube, P. (2013), "Contribution of record-keeping to audit opinions: an informetrics analysis of the general reports on audit outcomes of the Auditor-General of South Africa", *Esarbica Journal*, Vol. 32, pp. 52-61.

Ngoepe, M. and Ngulube, P. (2014), "The need for records management in the auditing process in the public sector in South Africa", *African Journal of Library, Archives and Information Science (October)*, Vol. 24 No. 2, pp. 135-150.

Ngoepe, M. and Saurombe, A. (2016), "Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African development community", *Archives and Manuscripts*, Vol. 44 No. 1, pp. 24-41.

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

Ngulube, P. (2005), "Research procedures used by master of information studies students at the university of natal in the period 1982–2002 with special reference to their sampling techniques and survey response rates: a methodological discourse", *International Information and Library Review*, Vol. 37 No. 2, pp. 127-143.

Nkala, S.G., Ngulube, P. and Mangena, B.S. (2012), "E-records readiness at national archives of Zimbabwe", *Mousaion*, Vol. 30 No. 2, pp. 108-116.

Office of Auditor General of Botswana (2008), The report of the Auditor General on Land Management: Performance Audit No. 2 of 2008, Government Printer, Gaborone.

Okello-Obura, C. (2012), "Records and information management as a conduit to effective auditing", *ESARBICA Journal*, Vol. 31, pp. 36-47.

Park, E.G. (2001), "Understanding 'authenticity' in records and information management: analysing practitioner constructs", *The American Archivist*, Vol. 64 No. 2, pp. 270-291.

Pinielo, I. (2015), "Auditor general reveals mess at air Botswana", available at: www.mmegi.bw/index.php?aid=49185

Porter, B., Simon, J. and Hatherly, J. (2003), *Principles of External Auditing*, Wiley, West Sussex.

Rajh, J.H.A. (2016), "The problem of maintaining and proving authenticity in the transition from producer to archive", available at: www.researchgate.net/publication/310450664_The_problem_of_maintaining_and_proving_authenticity_in_the_transition_from_Producer_to_Archive

Rezaei, N. (2013), "Enterprise resource planning (ERP) software implementation impacts on the auditing activities", *Journal of Applied Business and Finance Researches*, Vol. 2 No. 3, pp. 90-96.

Roeder, J., Eppard, P., Underwood, W. and Lauriault, T.P. (2008), "Authenticity, reliability and accuracy of digital records in the artistic, scientific and governmental sectors", available at: www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_3_domain2_task_force.pdf

Rogers, C. (2015), "Record authenticity as a measure of trust: a view across records professions, sectors, and legal systems", *INFuture2015: e-Institutions – Openness, Accessibility, and Preservation*, Vol. 13, pp. 109-118.

Rogers, C. (2016), "A literature review of authenticity of records in digital systems: from 'machine readable' to records in the cloud", available at: www.researchgate.net/publication/320593846_A_Literature_Review_of_Authenticity_of_Records_in_Digital_Systems_From_'Machine-Readable'_to_Records_in_the_Cloud/link/59ef72d1aca2722eb0be130e/download

Stancic, H., Ngoepe, M. and Mukwevho, J. (2019), "Authentication", in Duranti, L. and Rogers, C. (Eds), *Trusting Records in the Cloud*, Facet Publishing London, pp. 135-154.

Thanh, N.C. and Le Thanh, T.T. (2015), "The interconnection between interpretivist paradigm and qualitative methods in education", *American Journal of Educational Science*, Vol. 1 No. 2, pp. 24-27.

Tutorials Point (2015), "Systems analysis and design", available at: www.tutorialspoint.com/system_analysis_and_design/system_analysis_and_design_tutorial.pdf

Uganda Law Reform Commission (2004), "A study report on electronic transactions law", available at: www.ulrc.go.ug/sites/default/files/ulrc_resources/Electronic%20Transactions%20Law%20body_0.pdf

Uniting Church in Australia (2017), "Managing records in business systems guideline", available at: https://nswact.uca.org.au/media/4003/managing-records-in-business-systems-guideline.pdf

Further reading

Australia National Audit Office (2012), "Records management in the Australian public service", available at: www.anao.gov.au/sites/g/files/net1621/f/201112%20Audit%20Report%20No%2053.pdf

Gillath, I. (2020), "Audit trails: managing the who, what, and when of business transactions", available at: http://smartsheets.com/audit-trails-and-logs

Lauriault, T.P., Barbara, C.L., Taylor, D.R.F. and Pulsifier, P.L. (2007), "Today's data are part of tomorrow's research: archival issues in the sciences", *Archivaria*, Vol. 64, pp. 123-180.

MacNeil, H.M. (1998), "Trusting records: the evolution of legal, historical, and diplomatic methods of assessing the trustworthiness of records, from antiquity to the digital age", PhD Thesis, University of British Columbia, Vancouver.

Mosweu, T.L. (2012), "Assessment of the court records management system in the delivery of justice at the Gaborone magisterial district", Masters Dissertation, University of Botswana, Gaborone.

National Archives of Australia (2011), "Digital transition policy", available at: www.naa.gov.au/information-management/digital-transition-and-digital-continuity/digital-transition-policy/index.aspx

Ngoepe, M. and Ngulube, P. (2015), "A framework to embed records management into the auditing process in the public sector in South Africa", *Information Development*, pp. 1-14.

Nikolova, M. (2008), "Assessment the degree of e-communication between state administration, citizens and business", *Proceedings of the International Conference on Information Technology (Info-Tech 2008) 19 – 20 September 2008, Bulgaria*, Vol. 1.

Appendix. Interview questions for ICT professionals, auditors and records managers

1. What functionalities does GABS have to ensure that it creates and maintains authentic reliable digital records in the system?

2. From the controls embedded in GABS, to what extent do they have the ability to capture and protect the integrity and maintain authentic digital accounting records that are reliable and accessible as long as needed?

3. What criteria are used by auditors to conclude that digital records in information (such as) GABS have maintained their identity and integrity (authenticity) and reliability?

4. Has the authenticity of accounting records in GABS ever been in question during audits and rejected as evidence in the audit process?

5. Are instances where digital records have been rejected as evidence in the audit process and why?

6. Has Botswana National Archives and Records Services developed procedures (i.e. for storage media, physical care, metadata, etc.) for ensuring the maintenance of authentic reliable digital records created and stored in e-government information systems? Please explain further.

7. Has the Accountant General's Department developed procedures (i.e. for storage media, physical care, metadata, etc.) for ensuring the maintenance of authentic reliable digital records created and stored in e-government information systems such as GABS? Please explain further

8. What recommendations can you propose to ensure that e-government information systems such as GABS create and maintain authentic reliable digital records?

9. The following procedures are in place for the purposes of ensuring that digital records created and maintained in GABS remain authentic over time. Please tick all that apply.

About the authors

Olefhile Mosweu is currently a Postdoctoral Research Fellow at the University of Johannesburg, South Africa. He holds a Doctoral degree in Information Science from the University of South Africa and a Masters in Archives and Records Management from the University of Botswana. He has over the years worked in the public sector of Botswana as an archives and records management professional. He has authored several book chapters and articles in reputable publishing houses. He regularly reviews book chapters and journal articles in the eastern and Southern Africa region. He is an editorial member of the *Journal of the South African Society of Archivists*. He is a member of the Records and Information Association of Botswana, South African Society of Archivists and the Eastern and Southern Africa Regional Branch of the International Council on Archives. His research interests are archival education, digital records management, knowledge management and the impact of Industry 4.0 on records management. He was a Research Assistant and member of Team Africa in the International Research on Permanent Authentic Records in Electronic Systems project (InterPARES Trust) (2013–2018). Olefhile Mosweu is the corresponding author and can be contacted at: olfmos@gmail.com

Mpho Ngoepe is a Professor in the Department of Information Science at the University of South Africa (Unisa). Prior to his current position at Unisa, Prof Ngoepe has worked for the United Nations Children's Fund, Auditor-General South Africa and the National Archives of South Africa. Prof Ngoepe is serving in the national committee of the South African Society of Archivists (2009–2019) and the board of Eastern and Southern Regional Branch of the International Council on Archives (2009–2019) as the editor of the journals. He also serves on the advisory council of the National Archives of South Africa in his capacity as the chairperson of Gauteng Provincial Archives. He is the director of the African Team for the multi-national, interdisciplinary research project exploring issues concerning digital records called the International Research on Permanent Authentic Records in Electronic Systems (InterPARES Trust) (2013-2018).