TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACCA:	Association of Chartered Certified Accountants
ACL:	Audit Command Language
AGD:	Accountant General's Department
AGSA:	Auditor-General of South Africa
BNARS:	Botswana National Archives and Records Services
BOCRA:	Botswana Communications Regulatory Authority
CAATs:	Computer Assisted Audit Techniques
CCRCA:	Cybercrime and Computer Related Crimes Act
CPA:	Certified Public Accountants
DIA:	Department of Internal Audit
DIT:	Department of Information Technology
DPP:	Directorate of Public Prosecutions
ECM:	Enterprise Content Management
ECT:	Electronic Communications and Transactions Act
EDI:	Electronic Data Interchange
EFT:	Electronic File Transfer
GABS:	Government Accounting and Budgeting System
GAS:	Generalized Audit Software
GDN:	Government Data Network
ESARBICA:	Eastern and Southern Africa Regional Branch of the International Council on Archives
IAASB:	International Auditing and Assurance Standards Board
IDEA:	Interactive Data Extraction and Analysis
IFAC:	International Federation of Accountants
ISACA:	Information Systems Audit and Control Association
ICA:	International Council on Archives
ICT:	Information and Communication Technology
IFMIS:	Integrated Financial Management Information System
IRMT:	International Records Management Trust
ISO:	International Standards Organisation
MFED:	Ministry of Finance and Economic Development
NARA:	National Archives and Records Administration

NECCC:	National Electronic Commerce Coordinating Council
OAGB:	Office of the Auditor General of Botswana
PAA:	Public Audit Act
PAC:	Public Accounts Committee
PFMA:	Public Finance Management Act
SADC:	Southern African Development Community
SAI:	Supreme Audit Institution
UNCITRAL:	United Nations Commission on International Trade Law
UNISA:	University of South Africa
USAID:	United States Agency for International Development

LIST OF APPENDICES

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION OF RESEARCH PROBLEM AND ITS CONTEXT

1.1 Introduction

The world economy in the 1980s experienced global international and capital flows (Cameron 2013:401), which led to, among others, the deployment of computer systems to process financial and other data, and to perform, monitor and control their operational and administrative operations (Porter, Simon & Hatherly 2003:31). 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 2015:3). Conducting business processes in a digital environment meant that digital records were created. When it comes to accounting as a form of demonstrating accountability of the use of resources, including public monies, records remain a vital resource even in the midst of the noted developments. As such, auditors came to rely on computers as a tool for conducting auditing procedures (Porter et al. 2003:31) and for them to make audit opinions, they need authentic records (Bhana 2008:3; Ngoepe & Ngulube 2014:142). Without proper records of transactions, the objective of auditing, which is to ascertain the accuracy and reliability of financial statements and to possibly locate fraud, becomes difficult (Ngoepe 2004:8). This is also the case in the digital environment.

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, Seetharaman, Mohamed, Gopalan & San 2011:3523). For auditors to be effective, they have to use automated systems and understand the business purposes of the systems. Over and above that, it requires auditors to understand the environment in which the computer systems operate. The use of ICTs in auditing has effectively allowed auditors to increase their individual productivity, as well as that of the audit function (Moorthy et al. 2011:3523). One could say these technological developments in ICT usage in the workplace had a profound impact on auditing. Auditing depends on authentic records to thrive. Authenticity of records has to take into consideration the existing legislative framework.

Undertaking an audit of financial statements is a legal requirement in many countries. For example, in South Africa, the Public Finance Management Act (PFMA) makes it an obligation for public entities to submit their financial statements to the Auditor-General of South Africa (AGSA) for auditing within two months after the financial year has ended (Government of South Africa 1999). The notion holds true that without a records management programme in place, accounting officers would be unable to furnish the public audit oversight mechanism, in this case the AGSA, with current, reliable and accurate records of financial statements for auditing (Ngoepe 2004:8). A study by Ngoepe and Ngulube (2016:890) concluded that audit reports prepared by the AGSA 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 (2017:13) investigated the contribution of records management to audit opinions and accountability in government entities and it 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 (2012:37-38) reviewed 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 the management of records. 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).

Ngoepe and Ngulube (2014:136) 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 (1996:6) is of the view that proper financial management would be possible in organisations when there is adequate cross-reference between records management and accounting systems. Bhana (2008:20) succinctly puts it as thus:

> Any auditor will tell you that an ideal environment is where you can walk into an entity and you are provided with an audit file that contains the financial statements which are in turn cross-referenced to all the relevant supporting records in the same file or at least indicating where such records can be easily retrievable.

Such an ideal audit situation where a complete audit file with financial statements cross-referenced with available supporting records or indications of their location for retrieval would result in clean audit opinions (Ngoepe & Ngulube 2014:136). However, it is not always the case that evidence of transactions in the form of records is available to auditors during audits. Even when records are available, they may be incomplete, and their authenticity may not be guaranteed. In the digital environment, records authenticity is a major threat, as records are predisposed to being 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 (ISO 2016:7) and refers to its trustworthiness and the fact that it has not been tampered with or corrupted, either accidentally or maliciously (Duranti 2009:52). According to the National Archives of United Kingdom (2003:7), 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) (2000:7), 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 their structure has to be preserved. According to Rogers (2015a:19), modern societies rely very much on records for various purposes; hence, records management professionals acknowledge and identify records authenticity as necessary for their preservation.

Determining the authenticity of digital documents for purposes of auditing is problematic (Barrister 2006:19; Park 2001:288). In South Africa, for example, Mulaudzi, Mukwevho and Ngoepe (2015:2) 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 in order for them to support the audit process are not clear (AGSA 2014:68). In Botswana, the advent of e-government has ushered in the creation and use of digital records (Moloi 2009). Examples of these records include databases, word-processed documents, e-mail and websites. Others are converted from analogue to digital through imaging. Whether these records maintain their authenticity after creation is still a question that needs to be answered. Thus, one cannot be certain that auditors would accept them during their audit assignments.

The whole purpose of transacting public affairs in the digital environment is to make the delivery of public services more efficient. Nikolova (2008:100) observes that due to the availability of appropriate software applications, even those used for financial management, the majority of public sector transactions take place in a digital environment. 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). The records need to be assessed and analysed for their authenticity.

A study on Financial Records and Information Systems in the Accountant General's Department (AGD) in Botswana by the International Records Management Trust (IRMT) (2004a:47) revealed a lack of clarity among staff members about records management policies, procedures and responsibilities. Although the department's financial instructions and procedures stipulate which financial records should be kept and their retention periods, the document does not describe how accounting records such as payment vouchers and their supporting documents should be managed and preserved. Consequently, the IRMT (2004a:52) recommends that a records management policy and procedures should be developed in collaboration with the Department of Botswana National Archives and Records Services (BNARS). If the policy and procedures were in place, it would ensure an integrated approach to creating, maintaining, accessing, preserving and disposing both paper and digital records. The policy should cover the legislative and regulatory requirements relating to financial records management, definition of records and their key characteristics (such as evidentiary quality, authenticity, reliability), purpose of records (accountability and audit), requirements for record keeping and system design (paper and digital), standards for financial records management, skills and competencies for managing records, and user responsibilities (IRMT (2004a:52-53).

The IRMT (2004a:54) observes that records procedures need to support the conversion of data from paper records into the computerised Government Accounting and Budgeting System (GABS), which centrally manages government financial and accounting records. Computer data in the system are not easily accessible, as the accounting system is not designed for the management of, and access to, records over time. Furthermore, it is not easy to determine the authenticity of records in this system as some paper-based records such as invoices are scanned into the system without proper control. The IRMT (2004a:56) notes that auditors and external investigators are given onsite access to AGD records. Regarding the maintenance of the authenticity of digital financial records, the IRMT (2004a:57) cautions against the alteration or disposal of records by users without the support of documented records policy or procedures. Rogers (2015a:113) declares that the social indicators of records authenticity are written policies and procedures governing digital records, as well as retention and disposition schedules while technical records authenticity indicators are information about actions taken to preserve the digital records, access controls and audit logs. In Botswana's public sector, these policies and procedures are lacking. The IRMT (2004a:59) recommends that the Ministry of Finance and Economic Development (MFED) (the mother ministry of the AGD) should work with BNARS to ensure that the records management functionality is integrated into GABS so that it has a high reporting functionality to enable better digital records management. This study utilised archival diplomatics to explore the development of a framework for authenticating digital accounting records created and stored in GABS with the view to support the audit process in the public sector of Botswana.

This chapter specifically puts the study into context. It does that through providing the background to the study, statement of the problem, research objectives and questions, research methodology, scope and delimitation of the study, as well as an outline of the chapters for the study. Research on digital records management in the public sector of Botswana has been undertaken but those that specifically focused on accounting records created and stored by an integrated financial information management system, such as GABS, have not been identified by the researcher.

1.1.1 The uptake of ICTs in Botswana Government's Accounting Processes

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 1998:8; United States Agency for International Development (USAID) 2008; Mosweu 2012:7; Hendricks 2012). For financial management, this has seen the introduction of the Integrated Financial Management Information System (IFMIS) for purposes of promotion of efficiency, effectiveness, accountability, transparency, security of data management and comprehensive financial reporting (Hendricks 2012). Automation of auditing and accounting processes is done through implementation of business systems. The International Council on Archives (ICA) (2013:4) defines a business system as "an automated system that creates or manages data about an organisation's activities." They include applications such as those 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 2013a:4; Uniting Church in Australia 2017:3). According to the ICA (2013:4), business records typically contain "dynamic data that is commonly subject to constant updates (timely) are able to be transformed and holds current data (non-redundant)." Kastenhofer (2016:3) observes that business systems create and keep great quantities of digital records. Such systems are not necessarily equipped with capabilities for the medium and long-term preservation of records (McLeod 2012:191). 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 & Bowen 2005:132; Charles Darwin University, 2014:2).

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 Office of the Auditor General of Botswana (OAGB) (2007:6), GABS was implemented specifically to achieve the following:

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

GABS 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 & Bowen 2005:132; Charles Darwin University, 2014:2). Being a computerised information system, GABS generates digital accounting records. The system is described as a reasonably and well-developed information system (DFC Consortium 2013:20), a conclusion reached when the DFC Consortium undertook a Public Expenditure and Financial Accountability Assessment in Botswana.

1.1.2 The Audit Process

As a vocation, the practice of auditing the accounts of public institutions has a long history. It was there during the time of the ancient Egyptians, Greeks and Romans. During those days, checking clerks were appointed to check the public accounts (Institute of Company Secretaries of India 2014:321). Auditing came about due to the necessity to institute some system of inspecting and reporting on those whose responsibility it was to manage the wealth and monies of others (Mentz 2014:59). During ancient times, a steward or servant in charge of livestock, goods and other forms of wealth would periodically orally account to his master what he had done to protect and develop the wealth entrusted to him, and the master would listen to such oral accounts of stewardship (Whittington & Pany 2010: 8; Kritzinger 2016:17). The term "audit" comes from the Latin term "audire", which means to hear (Institute of Company Secretaries of India 2014:321). During the early days, persons used to listen to the accounts read over by an accountant in order to check them, the listener was the auditor (Institute of Company Secretaries of India 2014:321; Kritzinger 2016:17). The practice of accounting and the signs of its existence have been visible in ancient cultures such as Babylonia, Mesopotamia, Greece, Egypt and Rome (Ambashe & Alrawi 2013:95-96; Akinyemi, Okoye & Izedonmi 2015:15-18). Over time, accounting transformed from verbal accounts provided by stewards to a listening auditor to written or recorded transactions, which could be examined by the master. In Botswana, it is a legislative requirement for the accounts of expenditure of public sector bodies to be audited annually (Government of Botswana 2011b; 2012). This ensures that the use of state resources is accounted for as the delivery of public services is undertaken. It is for this reason that Gear (2013:15) opines that auditors have a responsibility to society. Auditors are expected to do a good job as an inaccurate audit or an audit failure can contribute to the collapse of large corporations that are running on capital supplied by banks and investors representing the public.

Audits serve a fundamental purpose in helping to enforce accountability and promote confidence in financial reporting. According to Ngoepe (2012:51), audits are undertaken as a measure to manage and confirm the correctness of an organisation's accounting procedures. Undertaking an audit of financial statements promotes accountability in the use of finances. An audit of financial statements refers to an independent examination of the financial statements of an organisation to enhance the degree of confidence of intended users in the financial statements (Certified Public Accountants Australia 2013:2). Through auditing, auditors perform a reasonable assurance engagement through providing an opinion on whether the financial statements present a true and fair view, and comply with accounting standards (CPA Australia 2014:7). An auditor expresses an opinion on whether the financial report is prepared, in all material respects, in accordance with an applicable financial reporting framework. To be in a position to express an audit opinion, the auditor follows a systematic process to obtain sufficient and appropriate audit evidence to support the resultant audit opinion (Essner & Unander-Scharin 2013:6; Kritzinger 2015:34).

For an auditor to express an opinion, a series of procedures and activities is performed to obtain evidence to substantiate the auditor's opinion (Ngoepe 2012:52; Mentz 2014:71). The auditor obtains audit evidence by means of a test of controls and substantive procedures that are sufficient (quantity of audit evidence) and appropriate (quality of audit evidence). This evidence refers to records. In conducting an audit, auditors follow various investigative processes and procedures in order to express an informed opinion on the veracity of an entity's financial and other information (De Jager 2008). The evidence consulted during an audit of financial statements has to be reliable so that it is acceptable for use to support the audit opinion arrived at by the auditor (Malaysian Institute of Accountants 2009:3). The evidence includes information contained in the accounting records underlying the financial statements and other information. The audit opinion expressed has to follow applicable financial reporting frameworks (IAASB 2015a:87).

Isa (2009:256) notes that organisations that place a higher commitment on the accountability process tend to have good record-keeping practices. This is mainly because auditors are aware that authentic and up-to-date records are key to their tasks. Through the audit process, the auditor adds credibility to management's financial statements, which allows owners, investors, bankers and other creditors to use them with greater confidence (Institute of Chartered Accountants in Australia 2008:2). Norman, Tobedza and Swami (2015:38) aver that a financial audit is a verification of the financial statements of an entity for purposes of expressing an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects. The opinion could also say that the audit results showed that the financial statements give a true and fair view in accordance with the financial reporting framework.

Prior to providing an audit opinion, an auditor has to observe the audit process, which has a number of phases. Phases of the audit process are presented in Annexure 1 at the end of this document. Elder, Beasley and Arens (2010:162) summarise steps undertaken in an audit of financial statements in four phases. These are briefly presented as follows:

a. **Phase I**: Planning and designing of an audit approach. This involves a study of the client's business strategies and processes. The auditor assesses the risk of misstatements in financial statements and evaluates internal controls and their effectiveness (Elder et al., 2010:162).

b. **Phase II**: Tests of controls and substantive tests of transactions are conducted.

c. **Phase III**: Analytical procedures and tests of details are performed. The auditor assesses whether account balances or other data appear reasonable and performs procedures to test for monetary misstatements in account balances.

d. **Phase IV**: Evidence gathered from accounting records and other sources of information is combined and an overall conclusion concerning the financial statements is formulated (Elder et al. 2010:63).

The audit process is documented in the form of an audit report in which auditors express an audit opinion (Becker Professional Education 2012:74-75; Dezan Shira and Associates 2013: 7). The specific types of audit opinions are presented in Table 1.1.

Table 1.1: Types of audit opinions (Becker Professional Education 2012)

Audit opinion	Explanation
Unqualified audit opinion	The financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with Generally Accepted Accounting Principles
Qualified opinion	Except for matters highlighted under the qualification, the financial statements present a fair view
Adverse	The financial statements do not present fairly the financial position, results of operations, or cash flows of the entity in conformity with Generally Accepted Accounting Principles
Disclaimer	The auditor does not express an opinion on the financial statements because he or she was not able to perform an audit sufficient in scope to render an opinion.

1.2.1 Auditing in an Information Technology Environment

The use of ICTs by businesses and governments has had a serious impact on accounting and audit processes (Nearon 2005:4; PricewaterhouseCoopers 2006:6; Abiola 2013:54; Abiola 2014:1739; Amatya 2016:84). The nature of digital evidence used to support an audit opinion requires an even greater level of scepticism than that for physical evidence due to the ease with which digital records can be altered without trail (Nearon 2005:4), making it problematic to prove the authenticity of digital documents for audit purposes (Park 2001). Comparatively, it is easier to detect the falsification of paper records than the falsification of digital records. Therefore, auditors have to exercise caution when auditing in a digital environment and not just rely blindly on evidence without weighing its sufficiency and competence (Nearon 2005:2). This raises the need to have clear criteria for determining whether digital records are authentic and reliable to support the audit process (Mukwevho & Jacobs 2012; Auditor-General of South Africa 2014). In fact, in a study of e-government readiness in the public sector of Botswana, Moloi and Mutula (2007:113) concluded that the greatest challenge in managing digital records produced by e-government platforms in Botswana lies in the management and preservation of such records as evidence of business transactions, a situation which could result in large informational gaps between e-records and paper-based records, leading to incomplete public records. For audit purposes, such potential gaps may render resultant digital records not being accepted in the audit process because auditors need authentic records in order to make audit conclusions (Ngoepe & Ngulube 2014:142).

The use of ICTs to conduct business processes affected the auditing profession and audit processes, requiring auditors to be adept in both information technology (IT) and auditing in order to keep up with technological developments (Carroll 2006:1). The computerisation of business records and the availability of computer-aided audit tools mean that these activities can be performed faster and more thoroughly. However, auditing in a digital environment needs to be supported by an appropriate regulatory and legislative framework. This is because legislation has a tremendous impact on how records, including those that are created and stored in networked environments, are managed (Ngoepe & Saurombe 2016:24). Countries such as Botswana, South Africa, Uganda and Mauritius have legislative frameworks that recognise the use of digital records in the transaction of public services (Government of Mauritius 2000; Government of South Africa 2002; Uganda Law Reform Commission 2004:49; Government of Botswana 2014a). The legislative framework that demands accountability in the use of public funds and resources in Botswana, of which auditing forms a part, includes the Constitution of the Republic, Public Audit Act and Public Finance Management Act (Government of Botswana 1966: 2011a: 2012). The national constitution established the Office of the Auditor General and mandates it to audit the accounts of all public bodies in Botswana. Specific functions of the Auditor General are detailed in the Public Audit Act (PAA) (Government of Botswana 2012). These pieces of legislation make it mandatory for public sector organisations to account for their actions and decisions with regard to public funds. An audit is usually performed to fulfil this obligation. The PAA requires the Auditor-General to audit the accounts and prepare the financial statements of public bodies as specified in the PFMA. According to the IRMT (2004a:53), the AGD views this regulation as the prime directive for good records management within the department.

As a whole, Nkwe (2012:129) concludes that because of deploying ICTs for public finance management in Botswana's public sector, technologies like electronic data interchange (EDI), image processing and electronic file transfer (EFT) have altered the audit process, as traditional audit trails will eventually be no more. Traditionally, auditors depended very much on source documents in paper form. The use of ICTs in financial information management compels auditors to audit online systems (such as GABS) and to use online audit software as their primary audit tool and gather evidence digitally.

1.2.2 The Relationship Between Records Management and Financial Accountability

Proper record keeping is a prerequisite for effective accountability (Meijer 2001:1; Abioye 2007: 61). In agreement with this assertion by these scholars, Isa (2009: iii) notes that the accountability of a government can arguably only be achieved when it demonstrates considerable transparency, which in turn can only happen when trust is supported by authentic and reliable records. Hurley (2005:224) who points out that in order to promote accountability, records must be complete, authentic, reliable, coherent, understandable and accessible, echoes a similar assertion. Similarly, Mentz (2014:70) argues that without reliable and authentic documentary evidence, the government cannot demonstrate to society that it has used state resources responsibly and that it has fulfilled its mandates.

Accountability is fundamental to good governance (Isa 2009:6). According to the IRMT (1999:6-7), accountability is the process that allows people to measure and verify the performance of the government. Financial accountability is a critical component of accountable government as, through relevant legislation, it institutes controls over budgets and accounts. Weaknesses in financial accountability are generally linked to weaknesses in public accounting, expenditure control, cash management, auditing and the management of financial records. An enhanced level of control over financial management is vital for all governments to maintain their commitment to their citizens. Isa (2009:68) notes that members of the public who elect their government through the ballot expect the government to be transparent and accountable. It is through its documented activities that records provide evidence of public administration and operations. An accountability process that is intimately related to the responsibility of the government mostly triggers the centrality of records.

1.3 Contextual setting of the study

This study attempted to design a framework to authenticate records in the government accounting system in Botswana to support the audit process. In order to put the study into perspective, it is necessary to illuminate the role played by major stakeholders in financial management processes, public sector auditing, records management and computerisation of government business functions.

The MFED manages state financial resources, coordinates the budgetary process and monitors expenditure. The European Commission Delegation Botswana (2009:7) notes that revenue generated by line ministries are transferred to the Consolidated Fund. All expenditure is incurred through a centralised payment system. This arrangement provides effective control over the extent of extra budgetary expenditure by the line ministries that can be incurred. The budgetary process is based on budget ceilings on an annual fiscal forecast. The budgetary process occurs within a pre-announced resource envelope and has strong bottom-up elements from the budget entities. Botswana adopts a dual budgetary process with both the recurrent and capital budgetary process coordinated by MFED (European Commission Delegation Botswana 2009:8). MFED performs some of its mandate through the AGD.

The use of government financial resources has to be in line with budgeted provisions. The Department of Internal Audit and the Office of Auditor General of Botswana (OAGB) provide internal and external audit services on an annual basis. In terms of the PFMA (Government of Botswana 2014) and the PAA (Government of Botswana 2012), the Auditor-General is empowered to conduct an audit of government financial statements annually. The GABS is used to manage the accounting and budgetary process. Thus, the Auditor General annually audits expenditure as transacted through the system. An audit of government accounts relies on available financial records. The fact that the records are created and stored in GABS means that BNARS and the DIT departments, that are mandated to manage public sector records and coordinate the computerisation of government ICT-based projects, are important stakeholders in the perspective of the study. The following section provides details of the major stakeholders necessary for resolving the research question of this study and these stakeholders are:

- Office of the Auditor General of Botswana (OAGB)
- Accountant General's Department (AGD)
- Botswana National Archives and Records Services (BNARS)
- Department of Information Technology (DIT)
- Department of Internal Audit (DIA)
- Department of Corporate Services at MFED

1.3.1 Office of the Auditor General of Botswana

The performance of audit functions of the Republic of Botswana predates independence. From the colonial period up to 1964, the Audit Office, as it was commonly known, had its head office in Pretoria, South Africa. Pretoria was the headquarters of the High Commission Territories (Bechuanaland Protectorate, Basutoland and Swaziland) (Rakgailwane 2004:30; Gustavson 2013:108). Each territory had a Senior Auditor. The Senior Auditor for Bechuanaland

Protectorate was based in Mafikeng, which served as the seat of government and administrative capital (Gustavson 2013:108). The audit office was moved to Gaborone in what came to be known as the independent country of Botswana in 1965 (Rakgailwane 2004:30). The head of the Audit Office was known as the Director of Audit until 1970, when the title of the post was changed to Auditor General (AG). The office focused primarily on financial audits, which addressed the accuracy, completeness and timeliness of financial statements. Audit activities were carried out manually and there was little planning with regard to such issues, as the audit approach or the qualifications of the staff needed to be engaged in the audits.

Almost all countries around the world have an established national auditing agency, monitoring the performance of the entire public sector in their country (Gustavson 2015:4). Globally, they are generally referred to as supreme audit institutions (SAIs). The OAGB is a constitutional office established as a public audit office by section 124 of the Constitution of Botswana, which provides that there shall be an Auditor General and a public audit office. The Auditor General is appointed by an Act of Parliament, which is ratified by the President, in accordance with the Constitution and the PAA (Government of Botswana 2012). The Auditor General is empowered to examine the accounts of all ministries, departments, local authorities, councils, land boards and parastatals (Rakgailwane 2004:30; Government of Botswana 2012). The duties of the Auditor General in terms of section 124(2) (and 3) of the Constitution of Botswana are to ensure that reasonable precautions are taken to safeguard the collection, receipt, issue, custody and disbursement of public monies and supplies in accordance with applicable laws and instructions. This piece of legislation empowers the Auditor General to audit the accounts and financial statements of public bodies, as specified in the PFMA (Government of Botswana 2011b). As part of its functions, the OAGB reports to Parliament by tabling reports of its audit findings to the Public Accounts Committee (PAC).

The PAC and SAIs such as the OAGB in the context of Botswana make a very important contribution to financial accountability and the stewardship process by providing to Parliament and the PAC independent reviews, information, assurance and advice on the accounts presented by the executive (Ngozwana 2009:3). This enables the PAC, on behalf of its Parliament, to undertake informed oversight. The SAI audits the accounts of government departments and other public institutions and submits its audit reports to Parliament. Parliament refers these audit reports to the PAC for detailed analysis and further investigations by calling relevant government officials to provide evidence before the committee. The objective of this process is to identify cases of inefficiencies and mismanagement, establish the root causes and develop recommendations for improvement. Key actors in accountability and the financial scrutiny cycle are Parliament, the executive, the SAI and the PAC. Ultimately, all these institutions have a combined responsibility (through Parliament) to provide assurance to voters that their tax money is being spent in a proper way. The OAGB is part of the study because its main function is to audit government entities, including a financial audit of financial statements created and stored by government accounting systems.

1.3.2 Ministry of Finance and Economic Development

The MFED is mandated with to coordinate national development planning, mobilisation and prudent management of available financial and economic resources. Additionally, the MFED formulates economic and financial policies for sustainable economic development. It undertakes its mandate through the following functions:

- treasury and budget administration
- economic management and national development planning coordination
- financial administration and management

The above functions are performed by the following divisions:

- Development and Budget Division
- Accountant General’s Department
- Economic and Financial Policy Division

The performance of the core mandate as depicted above is supported by the Department of Corporate Services. It consists of Human Resources Management, Office Administration, Information Technology Unit, Development and Finance, Procurement Unit, and Legal Services Unit. The MFED was selected to take part in the study because it is a policy-making body on public financial management. It is also where policy issues that affect IT and records management are approved. It is the mother Ministry of the AGD, which an implementing agency for GABS.

1.3.3 Accountant General's Department

The demands for accountability, transparency and good governance are reflected in the PFMA (Government of Botswana 2011b). This Act prescribes the duties of the Accountant General, a public officer entrusted with the compilation and management of government accounts, custody and safety of public moneys, and its disbursement. Section 42 of the Act empowers the Auditor General to audit public accounts within six months of the close of each financial year. The AGD is a department within the MFED. The department has a presence in all government ministries as well as independent government departments, in the form of an Accounting Unit. Officers work on secondment in the host Ministries overseeing the overall financial and budgetary control of expenditure. The AGD participates in the study as it is the custodian of GABS, an information system used for government accounting and budgeting functions.

1.3.4 Department of Botswana National Archives and Records Services

Through the National Archives and Records Services Act, BNARS is responsible for the management of public sector records and archives in Botswana, regardless of format or media (Government of Botswana 1978; Ngoepe & Keakopa 2011:155). Specifically, the department is entrusted with making provisions for the preservation, custody, control and disposal of public records and archives. The mandate of the department was extended to include the management of digital records through an amendment of the legislation in 2007. The amendment extended the definition of a record to include digital records. The mandate of BNARS includes providing an advisory role in records management among state-owned enterprises, commonly known as parastatal organisations in Botswana. BNARS is a department within the Ministry of Youth Empowerment, Sport and Culture Development. BNARS participates in the study because it is mandated to manage public sector records, including digital records created and stored within information systems such as GABS.

1.3.5 Department of Information Technology

The DIT was formerly known as the Government Computer Bureau (GCB). It evolved from the AGD. The government recognised the need for the computerisation of its functions long ago when, in 1966, the processing of payroll and accounting was undertaken using accounting machines in the AGD (Ojedokun & Moahi 2006:80). In 1969, ICT punched card tabulators replaced these accounting machines. The AGD later became the IT department of the GCB and an independent department in 1972. The department was transferred from the Ministry of Finance and Development Planning to then Ministry of Communications, Science and Technology in 2002 and is now a part of the Ministry of Transport and Communications (Government of Botswana 2011a).

The mandate of the DIT is to facilitate and administer information and communication technology services across the public sector. It advises government departments and ministries in all matters pertaining to ICT-related matters (Government of Botswana 2011a). It also provides website hosting services for government, e-mail connectivity and internet access. It outsources some of its functions and manages third-party agreements, which include the maintenance of the microcomputers in government ministries and departments. It has the following core divisions:

- Infrastructure Services Support (ISS)
- Ministry Support Services (MSS)
- Projects

- Strategy

According to Moloi (2009:116), the DIT plays a crucial role in government computerisation projects through providing an advisory role and setting standards that have to be met, from tendering to actual implementation. Scholars such as Moloi (2009), Mosweu (2012), and Ojedokun and Moahi (2006) identify several information systems coordinated and implemented over the years by the DIT as:

- Government Accounting and Budget System (GABS)
- Computerised Personnel Management System (CPMS)
- Social Benefit, Registration and Reconciliation System (SBRRS)
- National Registration System
- Court Records Management System (CRMS)
- National Archives and Records Management System (NARMS)
- Payroll System
- Livestock Identification and Trace Back System (LITS)
- Automated System for Customs Data (ASYCUDA)
- Vehicle Registration System
- Taxpayer Management System
- Water Resources Information System
- Teacher Management System (TMS)
- Student Selection System (SSS)

The DIT was included in the study as its mandate is to facilitate and coordinate the implementation of government computer-based information systems projects (Moloi 2009:112).

1.3.6 Department of Internal Audit

As a department within the MFED, the DIA helps in the achievement of accountability and transparency in the Botswana Public Service, not just the mother ministry (Government of

Botswana 2017a). The departments provide quality internal audit services to the Government of Botswana through adherence to the Standards for the Professional Practice of Internal Auditing and advises the management of the MFED and the rest of government entities (through seconded officers) on the following:

- The review of risk management, control and governance process.
- The maintenance of proper accounting records of government revenues and expenditures.
- The existence of adequate and effective controls, financial and otherwise.
- The need to review systems and procedures pertaining to management.
- Adherence to laid down laws, policies, procedures and guidelines.
- The economy, efficiency and effectiveness with which government resources are employed to ensure that the government receives value for money.
- The need to be gender sensitive in all aspects of their operations (Government of Botswana 2017a).

The DIA was selected to take part in the study because its mandate includes carrying out internal auditing services in Botswana government departments and ministries. This includes GABS as a system for financial management and control and is situated in the AGD.

1.4 Statement of the Problem

The state of affairs about determining the authenticity (in a financial audit) of digital accounting records created and stored in GABS, particularly for supporting the audit process, is yet to be determined. This situation is not peculiar to Botswana, as in the South African public sector, digital records have often not been accepted as evidence to support audit queries (Mulaudzi et al. 2015:2). Often, it is difficult to prove the authenticity and reliability of records consulted during audits. It is not clear as to how auditors conclude that records, especially digital records, are authentic and reliable (Park 2001:271; Barrister 2006:5-6; AGSA 2014). Comparatively, digital records may be more easily destroyed or altered than paper records without leaving any trace (International Auditing and Assurance Board 2010:229). According to the Australian National Audit Office (2012:86), achieving good records management in modern, complex business requirements and many digital business systems is highly challenging. The volatile digital environment poses risks that such systems might generate inaccurate or incomplete information, which is then accessed and used when making decisions, including during audits and service delivery. Archival legislation is also weak as far as digital records management is concerned. Except for South Africa, archival legislation in the Southern African Development Community (SADC) generally lacks the steel to regulate digital records management (Moloi 2009:113; Ngoepe & Keakopa 2011:155; Ngoepe & Saurombe 2016:37). Furthermore, for Botswana, records management professionals are poorly equipped to play a meaningful role in the management of digital record-keeping systems (Moloi 2009:113; Ngoepe & Keakopa 2011:155).

ISO (2016:4-5) indicates that organisations should create and maintain authentic, reliable and usable records, and protect the integrity of those records for as long as required, in order for them to support the continued flow of business, comply with the existing regulatory environment and provide the necessary accountability. This applies to both manual and digital records.

During performance audits carried out by the OAGB in the public sector, the audit process became questionable and unreliable for making worthwhile audit opinions, because available records were not authentic (OAGB 2008:35; Mosweu 2011:113; 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 International Auditing and Assurance Board (2010:229) points out that for records authenticity to be ensured, an organisation has to put in place information security policies, procedures and security controls in order to prevent unauthorised changes to records in the accounting system or to systems that provide data to the accounting system. In addition, auditors rely on automated controls, such as record integrity checks, digital date stamps, digital signatures and version controls when considering the integrity of digital evidence (International Auditing and Assurance Board 2010:229). The auditor may also perform additional procedures such as confirming transaction details or account balances with third parties during assessments.

This study therefore sought to propose a framework to guide the authentication of digital records particularly to support the audit process in the public sector of Botswana if the AGD adopted such a framework.

1.5 Aim and Objectives of the Study

A research aim usually precedes a series of statements describing a project's research objectives (Thomas & Hodges 2010:38). The research objectives are more detailed as they indicate specific research topics the study seeks to investigate, thus providing building blocks on the main theme stated in the research aim. In view of the aforementioned, this study sought to develop a framework for the authentication of records in a government accounting system in Botswana with the view to supporting the audit process in the public sector. This is done with the aim of ascertaining the current state of affairs in order to recommend the necessary interventions needed for enabling records management practices in a digital environment to support audit processes for accountability by in the Botswana public sector. The following objectives guided the study:

1.5.1 To analyse the legislative framework for the creation of authentic, reliable digital records stored in GABS in support of audit processes in the public sector of Botswana.

1.5.2 To find out what procedures are in place to maintain the authenticity of digital accounting records created and stored in GABS.

1.5.3 To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS.

1.5.4 To determine how digital records created and stored through GABS are managed as authentic to support audit processes in the public sector of Botswana.

1.5.5 To propose a framework to authenticate digital records created and stored in GABS to support audit processes in the public sector of Botswana.

1.6 Research Questions

To achieve the study objectives and find answers to the research problem, the following research questions were asked:

1.6.1 What legislative frameworks govern the creation of authentic, reliable digital records stored in GABS in support of audit processes in the public sector of Botswana?

1.6.2 What procedures are in place to maintain the authenticity of digital accounting records created and stored in GABS?

1.6.3 Which skills and competencies are needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS?

1.6.4 How are digital records created and stored through GABS managed as authentic to support audit processes in the public sector of Botswana?

1.6.5 What framework can be proposed to guide the authentication of digital records created and stored in GABS to support audit processes in the public sector of Botswana?

1.7 Conceptual Framework

The purpose of a conceptual framework is to define the research problem, establish theoretical coherence, organise the research design and implementation, and frame conceptual conclusions (Berman 2013:2-3). According to Lester (2005:460), “a conceptual framework is an argument that the concepts chosen for investigation, and any anticipated relationships among them, will be appropriate and useful given the research problem under investigation.” For Maxwell (2013:39), a conceptual framework is a constructed “tentative theory of the phenomena” used by the researcher to explain phenomena investigated. The concepts provide a lens through which the issue under investigation can be examined. It was imperative for this study to be anchored on a conceptual framework because empirical research should be guided by a theory to guide its choice of research questions, research methodologies and data analysis (Ngulube, Mathipa & Gumbo 2015:47). A theoretical framework guides good and successful research (King, Keohane & Verba 1994:29; Grant & Osanloo 2014:12). Such research is taken seriously and respected (Pettigrew & McKechnie 2001:62). Ngulube (2018:1) underscores the importance of a conceptual framework by saying that it is the glue that binds social research together such that without it, the whole research design crumbles. Therefore, as a directional pointer for research, it is impossible to separate research from theory. Ngulube (2018) adds that undertaking an empirical research without either a conceptual or theoretical framework is inconceivable.

The conceptual framework guiding this study resonates well with policy requirements for managing records. According to the IRMT (2004a:52-53), the legislative and regulatory requirements for managing financial records, the definition of records, including their key characteristics (evidentiary quality, authenticity, reliability), the purpose of records (accountability and audit), the requirements for record-keeping and system design (paper and digital), the standards for financial records management, skills and competencies for managing records, and user responsibilities are all part of a policy for records management.

The conceptual framework guiding this study was developed from the theory of archival diplomatics. Archival diplomatics provides a specified view of a model record and the means of understanding and defining record authenticity, including the elements that comprise it (McKemmish & Gilliland 2013:101). In order to protect the authenticity of records in digital systems, their identity and integrity need to be intact (Rogers & Tennis 2013:802; Duranti 2014). The same metadata are used to authenticate digital records (Tennis & Rogers 2012:41; McKemmish & Gilliland 2012:106). The metadata should be related to the records' content, structure and context as professed by Bearman (2007:18). According to Duranti (2014), archival diplomatics concerns itself with defining and assessing the trustworthiness of digital records or their authenticity. Archival diplomatics provided the foundation for the development of the study conceptual framework. In the digital environment, the internal and external elements that constitute a record such as context (juridical, administrative, procedural and documentary framework) in which the record is created, archival bond (which links the current record and the one before as well as the one coming after) and persons (entities acting by means of the record) are included as metadata in a digital information system (MacNeil 2000a:91-95; Duranti, Eastwood & MacNeil 2002:12-20).

InterPARES formulated archival diplomatics through the integration of traditional diplomatics with concepts and principles from Archival Science (Jansen 2014:40). These two are complementary. While diplomatics examines records as single entities in order to identify the characteristics embedded in the records themselves, Archival Science treats them as aggregates of the whole, thus examining their relationships to other records, to the persons involved in their creation and to the activities in the course of which they are created and used (Duranti & Thibodeau (2006:16). This study therefore used archival diplomatics to develop the conceptual framework that guides this study. The constructs that make up the conceptual framework are legislation, skills and competencies, management of records and procedures for records authenticity.

The construct of authenticity comes from archival diplomatics. This is supported by Kumar (2005:37) who argues that a conceptual framework "stems from a theoretical framework and concentrates, usually, on one section of that theoretical framework which forms the basis of a research." The conceptual framework underpinning this study is presented in Figure 1.1 in line with Ngulube et al. (2015) who suggest that a conceptual framework is best depicted diagrammatically. Thereafter, each of the constructs in the conceptual framework is explained.

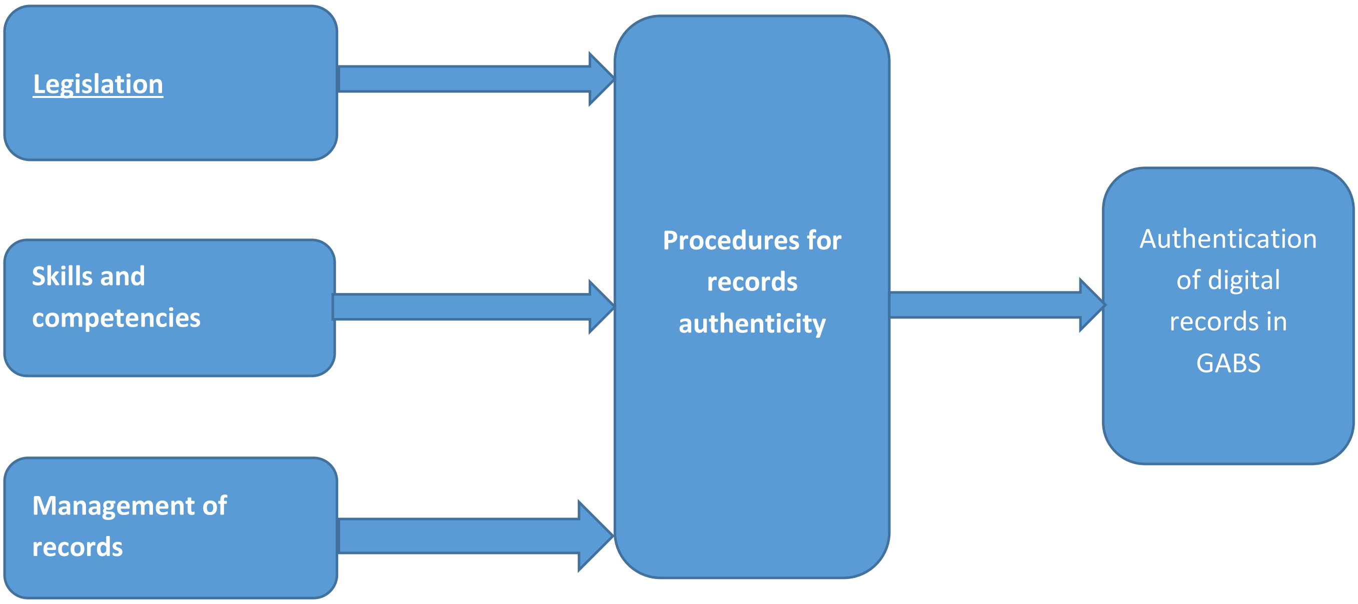

Legislation
Skills and competencies
Management of records
Procedures for records authenticity
Authentication of digital records in GABS

Figure 1.1: Conceptual framework for the study

1.7.1 Legislation

Both records management and auditing take place within a framework of laws for guidance, even in the digital environment (Bantin 2008:233). Principally, the National Archives and Records Services Act and other laws such as the Electronic Records (Evidence) Act (Government of Botswana 2014a) regulate public sector records management in Botswana. It recognises digital records as evidence in legal proceedings. The Electronic Communications and Transactions Act also support digital records management in the networked environment. It prescribes for the authentication of digital records using digital signatures and these should not be denied legal effect simply because they are in digital form (Government of Botswana 2014b). The Cybercrime and Computer Related Crimes Act makes the interception and forgery of data in computer-based information systems illegal (Government of Botswana 2007). The PAA empowers the Auditor General to audit public finances annually (Government of Botswana 2012) in accordance with the provisions of the PFMA (Government of Botswana 2011b). The Constitution of Botswana provides for an overall accountability for the use of state resources in a transparent manner.

1.7.2 Procedures for Records Authenticity

Authentic records are those that are trustworthy as records and claim to be what they purport to be and are free from tampering or corruption (Duranti 2001:44). Notably, records in the digital environment are at risk of being easily tampered with or corrupted, either accidentally or maliciously (Bradley 2005:166; Duranti 2009:52). Records that are authentic are those whose identity and integrity metadata have been protected (MacNeil 2004:200-201). The authenticity of digital records can be maintained through employing social and technical procedures. Social indicators of records authenticity are written policies and procedures governing digital records, retention and disposition schedules, while technical records' authenticity indicators are general IT controls and system application controls (Rogers 2015a:113). Authentic records are required in the audit process to formulate audit opinions (Bhana 2008:3; Ngoepe & Ngulube 2014:142). There are a number of records authentication technologies that can establish the authenticity of digital records and these include digital signatures, timestamps, hash digests, checksums and cyclic redundancy checks, among others (Elliot 2007:2).

1.7.3 Skills and Competencies

The management of records in a digital environment needs skilled and competent records management professionals. A lack of capacity to manage digital records is a weakness in the ESARBICA region, Botswana included (Kemoni 2009:194; Katuu & Ngoepe 2017:22; Oganga 2016:67). The National Archives of Australia recognised the need for competencies for records management and ICT professionals by documenting them in its Digital Continuity

Policy Competency Framework (National Archives of Australia 2015). The capabilities and skills needed by archives and records management, and ICT professionals to confidently manage digital records and thus authenticate them, have been listed at Table 2.1 in Chapter Two.

The need is also true for auditors who undertake financial audits in the networked environment (Carroll 2006:63; Moorthy et al. 2011:3524). Accordingly, an auditor should be able to perform tasks required to start and complete an audit engagement. Legislation requires that auditors should have a high level of professional competencies in order to offer reasonable assurance that the financial statements of an audited entity truly and fairly represent its financial position (Gear 2013:15). According to the Chartered Accountants Australia and New Zealand (2016:3), some of the competencies needed for a financial audit include planning the audit, risk assessment, internal review control, substantive testing, documentation and forming an opinion, staff supervision and audit management, decision-making on reporting and other issues, and application of the knowledge of auditing standards as well as appropriate legislation. Auditor competency and expertise are factors that affect the quality of an audit (Gear 2013:22).

1.7.4 Management of Records

Records as documentary evidence of organisational functions should be managed across their entire life cycle, including those created in digital systems. Records are to be understood in the context of their creation, which is the framework for action (Reed 2005:41; Duranti & Rogers 2012:524). As by-products of the performance of business activities, records need proper management to enable their evidentiary value to stand. This evidentiary value is sustained right from the time the records are created, through its use and can be validated and reasoned about by authorised users. A determination can be made through checks to ensure that it has not been modified, abused or tampered with (Ma, Abie, Skramstad & Nygård 2009:2). Management activities include proper storage, records safety and security, assigned responsibilities for their management, guidance in the form of records management policies and procedures, and records retention and disposal. The management of records is linked to legislative and regulatory requirements (IRMT 2004a:53). For example, the repealed Finance and Audit Act, which has been replaced by the PAA (Government of Botswana 2012), issued the Financial Instructions and Procedures (Government of Botswana 1993), which stipulates retention periods for selected records that range from three years to 10 years. The accounting and auditing functions rely on properly kept records, otherwise proper financial management becomes impossible (World Bank/IRMT 2000:6).

1.8 Justification and Originality of the Study

Originality in a doctoral thesis has been considered essential for more than a century (European Universities Association 2010:3; UK Quality Assurance Agency for Higher Education 2015:4) for purposes of achieving ‘doctorateness’ (Wellington 2013:1493). Guetzkow, Lamont and Mallard (2004:190) point out that originality in research in humanities and social sciences is defined as encompassing “the use of a new approach, theory, method, or data; studying a new topic, doing research in an understudied area; or producing new findings.” The originality of this study stems from a new research topic investigated through a conceptual framework developed from archival diplomatics. This study is also interdisciplinary as it includes records management and auditing, with a special focus on assessing authenticity and reliability of digital records in an integrated financial information management system (i.e. GABS). It may contribute to policy development in the two disciplines (Ngoepe 2012). This study complements other studies conducted in Namibia, Nigeria, Zimbabwe, Kenya and Tanzania, but those focused on the management of financial records and did not place focus on authenticity of digital accounting records to support the audit process (IRMT 2001; 2002; 2004a; Malemelo, Dube & David 2013:12). This study is also justifiable because it recommended a framework that can be used to guide audit processes based on authentic reliable digital accounting records created and stored in GABS.

1.9 Significance of The Study

Creswell (2003:149) says that the significance of the study elaborates on the importance and implications of a study for researchers, practitioners and policymakers. This study is significant in several ways. For BNARS, its findings stand to illuminate the capability of digital accounting records produced and stored in GABS to support public audit processes. The findings are capable of informing policy development and implementation fit to support audit processes in a digital environment. Secondly, this study will propose a framework for ensuring that authentic, reliable records are created and stored in GABS to support audit processes in the public sector of Botswana. The beneficiaries of the framework will be BNARS, the AGD, and the Office of the OAGB and Government Ministries. The framework would serve more like an evaluative tool in guiding the creation and maintenance of authentic digital accounting records. Archivists and Records Managers in similar socioeconomic environments, particularly in Africa, are likely to use the proposed framework to help guide the management of authentic accounting records in a digital environment. Generally, the study stands to add to scholarly literature digital records in general and authentic reliable digital accounting records in particular.

1.10 Motivation for the Study

This research topic was motivated by a lack of empirical studies focusing on investigating the authenticity and reliability of digital records in support of audit processes in the public sector of Botswana. This study has been successfully carried out as planned. It has added new knowledge in the area of authenticating digital records to support the audit process. This study has the potential to come up with practical solutions as it links the need for authentic and reliable digital records to support audit processes. This is particularly important as the Government of Botswana has an active e-government programme whose adoption has resulted in digital records as and when public affairs are transacted. Records through an audit process facilitate assessing accountability in the delivery of public services. Available empirical studies of digital records management in the public service of Botswana have focused on records management issues arising from performance audits, probed and examined factors affecting the adoption and use of electronic and document records management systems, digital records management, management of e-mail, e-records readiness and digital court records management systems (Moloi & Mutula 2007; Keakopa 2008; Mosweu 2012; Moatlhodi 2015; Mosweu, Bwalya & Mutshewa 2016a; Mosweu, Bwalya & Mutshewa 2016b). None of the studies specifically focused on investigating the authenticity of digital records in support of audit processes, hence, this study. Insights from this study would be useful in enabling the sustenance of authentic and reliable digital records needed for accountability and transparency in the use of public resources, particularly that the Government of Botswana uses ICTs to deliver public services.

1.11 Scope and Delimitations of the Study

This study is limited to six purposively selected government departments. Local authorities and land boards are excluded as they both fall under a relevant ministry in administrative terms and they do not use GABS to manage financial records. These departments were selected because they were relevant in the endeavour to resolve the research question. The DIT and BNARS were selected because they are mandated to manage government computerisation projects and public sector records, respectively (Government of Botswana 1978; Moloi 2009:112). The OAGB is included as it is responsible for regularity auditing of public sector bodies in terms of the PFMA and the PAA (Government of Botswana 2011b:2012). The AGD is the principal study location and custodian of GABS. The Department of Corporate Services coordinates support services in the MFED and ministry records managers are based there. The Department of Internal Audit regularly performs internal audits in government entities and was included because its mandate includes an audit of implemented business systems.

This study focuses only on regularity auditing. In the context of Botswana, auditing firms and government undertake different types of audits such as statutory audits, non-statutory audits, external audits, internal audits, social audits and performance audits (Nkwe 2012:127). Regularity (or financial) auditing refers to an audit which is meant to ensure that systems of accounting and financial control are efficient and are operating properly and those financial transactions have been correctly authorised and accounted for (Zinyama 2013:268). It verifies that expenditure is incurred as planned and that it is in accordance with statutory and other regulations and authorities governing them. In this stance, a financial audit falls within the category of statutory audit because it is prescribed by both the PFMA and the PAA (Government of Botswana 2011b; 2012). According to the Controller and Auditor General of India (2016:2), compliance auditing is an assessment of whether there has been compliance with the provisions of the applicable laws, rules, regulations, orders and instructions issued by a competent authority. It is also called value-for-money auditing (Zinyama 2013:268). The other types of audits are not covered in this study, as they do not meet the requirements of regularity auditing. GABS monitors the expenditure of preapproved government finances, hence the inclusion of regularity audits. This study excluded other information systems deployed in the public service to facilitate the performance of various functions such as electronic document and records management systems (EDRMS) and others. The main reason for their exclusion was because the focus of the study was on a government-wide implemented system used for financial management, and GABS was the ideal one.

1.12 Definition of Key Terms

The definition of key terms and concepts used for this study is meant to provide the context in which they are used and understood. According to Saurombe (2016:22), defining terminology in research is very useful and relevant as it makes the concepts explored within the study more comprehensible. It also eliminates ambiguity as certain terms can vary in meaning due to the different contexts under which they are applied. The following terms and concepts form the working definitions as used in this study.

1.12.1 Digital Records

Different words are used to refer to the concept “digital record” and these are presented in literature as “electronic records” and “e-records”. All these constitute the same thing. This study has adopted the Australian definition of digital records, which defines it as “records created, communicated and maintained by means of computer technology” (National Archives of Australia 2004:13). Records may be either ‘born digital’ (created using computer technology) or digitised from their original formats (e.g. scans of paper documents).

1.12.2 Records Management

According to ISO 15489, records management is a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (ISO 15489-1: 2016). In the context of this study, records management refers to the practice of creating and maintaining records by an organisation (IRMT 2004b).

1.12.3 Auditing

RAFFA (2003:1) defines auditing as a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between those assertions and established criteria and communicating the results to interested users. The objective of an audit is to provide a reasonable basis for expressing an opinion regarding the financial statements taken as a whole. Financial statements are fundamentally an organised assembly of transactions presented in a manner that purports to represent the performance of an entity (Bhana 2008:2).

1.12.4 Authenticity

Authenticity refers to the trustworthiness of a record and its ability to demonstrate that it has not been tampered with or corrupted, either accidentally or maliciously (Duranti 2009:52). Authenticity of a record is assessed by establishing its identity and demonstrating its integrity

(Rogers 2015a:112). In the digital environment, a presumption of authenticity is an inference based on evidence about how the records have been created and maintained. Evidence may come from the records creator, or through further analysis to verify authenticity, such as a comparison of the records with copies preserved elsewhere (redundancy), forensic analysis, testimony of a third party or analysis of audit trails (MacNeil & Gilliland-Swetland 2005; Duranti & Thibodeau 2006; InterPARES 2008).

1.12.5 Authentication

The word authentication refers to a declaration of a record's authenticity at a specific point in time by a juridical person entrusted with the authority to make such a declaration (e.g. public officer, notary, certification authority) (InterPARES 2007:7). It can also be regarded as a certificate of authenticity whereby the records creator or preserver declares that one or more reproduced or reproducible digital records are authentic (InterPARES 2007:10). Duranti (2005:2) defines it as a declaration of authenticity that can be provided by any person responsible for keeping the original of a record or an official copy. According to Mason (2004:40), for a record or document to be authenticated, it must have the following characteristics:

a. **Reliability** – there is evidence that records are created and captured as part of the legitimate business process and that they are subject to a corporate management process.
b. **Integrity** – the document is protected from unauthorised alteration.
c. **Usability** – the document is capable of being retrieved, presented and interpreted correctly.

1.13 Research Methodology

This section presents the research methodology employed for this study. Research methodology refers to the way a research problem is resolved systematically (Kothari & Garg

2011:7). Research involves philosophical assumptions about the nature of the world, the way it is understood, and the distinct methods or procedures chosen (Rogers 2015b:74). This study is qualitative (Creswell 2014:32) and thus guided by interpretivism (Jupp 2006:342; Thanh & Le Thanh 2015:25), which, as an epistemology, is linked to constructionism, the meaning of which, as an ontology argues, is constructed through social interaction and is thus subjective (Lincoln & Guba 1985:37; Gray 2009:23). The main characteristic of qualitative studies is that they are conducted in natural settings with subjective meanings constructed from an understanding emanating from the minds of participants (Leedy & Ormrod 2005; Jupp 2006:249; Creswell 2007:37). This study adopted a single case study research design (Yin 2009:2; Creswell 2013:97).

The research problem and topic determine the research approach selected (Creswell 2014), because no single approach fits any problem (Ngoepe 2012:35). This study investigated the authentication of digital accounting records created through GABS in order to ascertain their authenticity for supporting audit processes in the public sector of Botswana.

The study population was made up of all 24 line ministries of the government of Botswana, including independent departments as identified from the 2017 Botswana Telecommunications Corporations (BTC) telephone directory (BTC 2017). Five departments were purposively selected based on their function and potential to resolve the research problem.

- BNARS: mandated to manage public sector records across their life cycle regardless of media or format.
- Department of Corporate Services in the Ministry of Finance and Economic Development.
- Department of the Accountant General: responsible for the compilation and management of government accounts, custody and safety of public moneys, and its disbursement, through GABS.
- Department of Internal Audit: provides internal audit services for government ministries and departments.

- Department of Information Technology: coordinates computerisation of government projects.
- Office of the Auditor General: audits government ministries and departments, including financial or regularity audits.

The participants were purposively selected to take part in the study. Both Tongco (2007:1470) and Palys (2008:697) aver that study participants can be selected because of their ability to provide answers to the questions posed. Data were collected from government entities. Meetoo and Temple (2003:1) and Ahmed and Sil (2012:935) advocate for a multi-method approach in research as it enhances the validity of research findings. Data were collected through documentary reviews and interviews.

1.14 Structure of the Thesis

Chapter One introduces the study and includes the framework of the study, problem statement, aim and objectives, definition of terms, justification and originality of the study, significance of the study, scope and limitations of the study, motivation of the study and a brief description of the research methodology. The purpose of the chapter is to present the background of the study and, at the same time, put it into context.

Chapter Two presents the literature review related to authenticity and reliability of digital records managed in information systems in the context of the public sector. The review is aligned to research objectives. The literature covers themes emanating from research objectives. They are an identification and analysis of the legislative framework for the creation of authentic, reliable digital records created and stored in accounting or financial information systems; criteria for the creation of authentic digital records; competencies and skills needed by auditors, ICT specialists and records managers to establish the authenticity and reliability of digital records created and stored through information systems and the management and preservation of digital records throughout their life cycle.

Chapter Three addresses the research methodology, including the research design and research methods. It specifically presents the research approach, the sampling technique employed and the population of the study, data collection instruments and data analysis techniques. It also presents ethical considerations put into practice during the conduct of the study.

Chapter Four presents the findings of the study. The findings are presented in accordance with the research objectives.

Chapter Five interprets and discusses the findings as presented in Chapter four. This is done through making observations and comparisons as found in literature. The purpose of the chapter is to bring to the fore an interpretation of the findings of the study as presented in Chapter four.

Chapter Six consolidates the study by summarising the research findings, concludes the study and makes recommendations for ensuring authenticity and reliability of digital records created through GABS in support of audit processes in the public sector of Botswana. It also proposes a framework that may be suitable for examining and understanding e-record readiness in labour organisations.

1.15 Chapter Summary

This chapter provided the background to the study. It has done so by putting the study into context and specifically presented the statement of the problem, study objectives and research questions, a description of the methods of investigation, and justified the investigation emanating from this study. It has also defined concepts used in the study. The next chapter presents the literature review related to the study.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The previous chapter introduced the study and provided a background of the study problem. Various scholars, including those in Library and Information Science (LIS), agree that a review of literature is a necessity in an empirical study for various reasons. Dilevko (2007:451) attests that a review of literature provides key building blocks for good research. Its purpose is to share with the reader the results of other studies closely related to the one being undertaken. It also relates to the larger, ongoing dialogue in the literature, filling in gaps and extending prior studies (Creswell 2014:61-62). It provides a framework for establishing the importance of the study as well as a benchmark for comparing the results with other findings (Creswell 2009:25-27). According to Randolph (2009:2), literature review is a means of demonstrating an author's knowledge about a particular field of study, including vocabulary, theories, key variables and phenomena, and its methods and history. It also informs students of the influential researchers and research groups in the field (Randolph 2009:2). Mertens (2010:90) explains that most of empirical studies are grounded on a review of literature from which the researcher is able to map the overall framework of the study at hand in terms of where it fits into the big picture of what is known about the topic from prior studies. Kumar (2005:30) states that from the inception of a study, it helps to establish the study's theoretical roots, clarify ideas and develop one's methodology. After data collection, the reviewed literature augments and consolidates the newly found knowledge base from findings and assists in the integration of findings with the existing body of knowledge.

This review of literature explores the central theme of this study, which is ensuring the authenticity of digital records in government accounting systems to support audit processes in the public sector of Botswana. It is organised in accordance with the research objectives of the study. It explores literature related to the context of the study with greater and specific focus on the legislative framework for the creation of authentic, reliable digital records, criteria used by auditors, ICT specialists and records managers to determine the authenticity and reliability of digital records created and stored through information systems, capabilities needed by auditors, ICT specialists and records managers to establish the authenticity and reliability of digital records created and stored in information systems and the management, preservation and storage of authentic, reliable digital records created and stored in information systems in support of audit processes in the public sector.

2.2 The Legislative Framework for the Management of Digital Records

Records should be managed through guidance of a specific regulatory framework, the purpose of which is to provide an environment that is conducive to proper records management. This includes managing records in a digital environment (ISO 15489 – 1: 2016:8; Bantin 2008:233; Okello-Obura 2011:6). Countries around the world have archival legislation that promotes the proper management of digital records; for example, Canada has the Library and Archives Act (Government of Canada 2004, amended in 2016), South Africa has the National Archives and Records Services Act (Government of South Africa 1996) and Sweden has the Archives Act (Anderson 2013:2). In most archival legislation, the definition of the word ‘records’ includes digital record. Botswana’s national archival legislation was amended in 2007 to include ‘digital record’ in its definition of a record (Ngoepe & Keakopa 2011:155). While Ngoepe and Saurombe (2016:29-30) acknowledge that the wide coverage of the definition of a record helps to ensure that as many forms of records as possible in as many media as possible are included, the legislation is still inadequate to deal with managing records in a cloud environment (Ngoepe & Keakopa 2011:155; InterPARES 2016:10). For example, Ngoepe and Saurombe (2016:29-30) conclude that as much as the Minister responsible for the archives and records management portfolio has the mandate to declare any place to be a place of deposit, the legislation is still inadequate in answering the following questions:

> Does the Minister have the capacity to determine such suitability? What are the legal obligations of having such a declaration? Does the Minister and Director have a legal capacity to monitor the cloud, and if there are violations in the

> cloud, can they charge those responsible for such violations? (Ngoepe & Saurombe 2016:30).

According to Adu (2015:25), the introduction of a legislative framework within the public sector is part of a larger framework for the management of public records. These manifest in the form of Acts, legislation and policies that give clear direction to the management of public records. According to scholars such as Ngulube and Tafor (2006:60), Hamooya, Mulauzi and Njobvu (2011:116), Okello-Obura (2011), Kalusopa (2011:228) and Ngoepe and Saurombe (2016:24), public records management operates within a framework of laws. In Botswana, several legislative instruments are applicable to the management of records in the country. These are the National Archives and Records Services Act, Electronic Records (Evidence) Act, Electronic Communications and Transactions Act, Public Audit Act, Public Finance Management Act, National ICT Policy and e-Government Strategy.

2.2.1 National Archives and Records Services Act Cap 59:04 Of 1978

Most of the national archival legislation in the Southern African Development Community (SADC) was enacted after independence and modelled along the United Kingdom's Public Record Act, in the case of Botswana in 1958, Portugal, former colonies, Mozambique and Angola (Mnjama 2014:30; Ngoepe & Saurombe 2016:29). Prior to the amendment of Botswana's archival legislation in 2007 to formally extend its legal mandate to the management of public sector records across their life cycle (Ngoepe & Keakopa 2011:155; Manewe-Sisa, Mooko & Mnjama 2016:156; Ngoepe & Saurombe 2016:29), the archives legislation only covered archives administration (Government of Botswana 1978). Almost all the literature available points to the National Archives Act of 1978 as the one that established archives and records management services in the country (Mbakile 2004:11; Keakopa 2006; Moloi 2009:109; Ramokate & Moatlhodi 2010:68) as shown by the cited few.

As amended in 2007, the management of public sector records in Botswana is now regulated by the National Archives and Records Services Act (Government of Botswana 1978). Its scope includes the management of digital records. Although this legislation recognises digital records as part of national heritage when they are included as archives, there are no guidelines as to how digital records should be managed to ensure that their authenticity and integrity are maintained for as long as they are used. Ngoepe and Keakopa (2011:155), and Moatlhodi (2015:74) have also indicated that the National Archives and Records Services Act is inadequate to regulate the management and preservation of digital records-keeping systems. The Electronic Records (Evidence) Act provides for the admissibility of digital records as evidence in legal proceedings and authentication of digital records (Government of Botswana 2014a). Ngoepe and Saurombe (2016:30) observe that section 5 of this Act indicates that, where a digital record is obtained from a digital records system and duly certified as such by the certifying authority in relation to the operation or management of the approved process, it shall be presumed that it accurately reproduces the contents of the original records system.

2.2.2 Electronic Records (Evidence) Act

Through the recently superseded long-term vision for Botswana, the National Vision 2016 (Government of Botswana 1997), and the National ICT Policy (Government of Botswana 2007), the country promoted the use of ICTs, particularly web-based applications to enhance access to and delivery of government information and services to citizens, business partners, employees, other agencies and government entities (Mosweu 2012:6). However, Kalusopa (2008:106) notes that, by 2008, the government still lacked appropriate legislation to deal with the ICTs that its policies were instituting, despite the fact the ICTs generated digital records (Moloi 2009:110). In view of both the Criminal Procedure and Evidence Act (Government of Botswana 2004) and the Evidence in Civil Proceedings Act (Government of Botswana 1977) providing for the admissibility of documentary evidence (without provisions for digital records), a need arose for enacting legislation to enable evidence contained in digital records to be tendered as evidence before the courts (Ganetsang 2015), in the form of the Electronic Records (Evidence) Act (Keetshabe 2012; Government of Botswana 2014a).

Therefore, the Electronic Records (Evidence) Act was enacted to provide for the admissibility of digital records as evidence in legal proceedings and authentication of digital records

(Government of Botswana 2014a). It also provides for the admissibility as evidence of digital records as original records. Ngoepe and Saurombe (2016: 30) observe that section 5 of this Act indicates that, where a digital record is obtained from a digital records system and duly certified as such by the certifying authority in relation to the operation or management of the approved process, it shall be presumed that it accurately reproduces the contents of the original records system. This legislation is well placed to promote the maintenance of digital accounting records. However, in the situation where GABS is not integrated with a digital records management system, maintaining the authenticity of digital accounting records within the system may be questionable, as GABS, although it produces and stores digital records, is not a purely digital records management system

2.2.3 Public Finance Management Act

The PFMA demands that accountability, transparency and good governance be reflected in all public sector financial management dealings (Government of Botswana 2011b). This Act prescribes the appointment of an Accountant General, a public officer entrusted with the custody and safety of public moneys, and its disbursement as well as the compilation and management of government accounts. The Act empowers the Auditor General to audit public accounts within six months of the close of each financial year. Although a proper records management regime is a critical element for the preparation of financial statements in organisations, as it facilitates the verification of the completeness and accuracy of data reported in the financial statements (Ngoepe 2012), Ngoepe and Ngulube (2013b:5) in a study that explored the role of records management in corporate governance in South Africa, found that the AGSA was not able to express an opinion on the financial statements primarily due to insufficient records.

2.2.4 Public Audit Act

The current PAA was initially part of the now defunct Finance and Audit Act of 1970 (Government of Botswana 1970) but it was replaced by the PAA (Government of Botswana

2012). The Finance and Audit Act also contained provisions now legislated in the PFMA (presented in detail in Section 2.2.3). Therefore, out of the provisions of the old Finance and Audit Act came the two laws: the PAA and the PFMA, separately.

The PAA provides for the Office of the Auditor General as established under the Constitution of the Republic of Botswana (Government of Botswana 2012) and outlines the duties of the Auditor General in terms of section 124(2) and (3) of the Constitution. These duties are to ensure that reasonable precautions are taken to safeguard the collection, receipt, issue, custody and disbursement of public monies and supplies, in accordance with applicable laws and instructions. This piece of legislation empowers the Auditor General to audit accounts and financial statements of public bodies as specified in the PFMA of 2011. In conducting the audits, the Auditor General must follow existing auditing standards, manuals or codes of ethics. Section 19(2a) of the PPA prescribes that the audit reports have to reflect at least an opinion or a conclusion on whether the annual financial statements of public bodies audited fairly present the financial position for the period covered by the audit.

The recognition of digital records in business transactions in the public sector requires appropriate mechanisms to ensure that they are authentic and remain reliable for as long as they are needed. Tafor (2003) and Stair and Reynolds (2006) caution that digital records are susceptible to easy manipulation, but they should remain available, usable, understandable and authentic for as long as they are needed. To avoid easy manipulation, digital records must be managed in a record-keeping system as they produce authentic and reliable records (South Carolina 2007:2). InterPARES (2008:40) defines a record-keeping system as a set of rules governing the storage, use, maintenance and disposition of records and/ or information about records, and the tools and mechanisms used to implement these rules. The legislative framework therefore should provide an environment that makes it practical to manage records in a digital environment, following records management principles. However, literature on records management in Botswana shows that the legislative framework lacks the capability to influence the proper management of digital records in Botswana (Ngoepe & Keakopa 2011:155; Ngoepe & Saurombe 2016:30).

2.2.5 Electronic Communications and Transactions Act

The internationalisation of markets and the realisation that the exchange of goods and services transcended jurisdictions promoted what is known as electronic commerce (e-commerce) (Botswana Communications Regulatory Authority (BOCRA) (2015:5). Through e-commerce, products and services could be sold worldwide using the internet as a medium, thus transcending foreign jurisdictions. According to BOCRA (2015:5-6), e-commerce was unattainable without a solid enabling legal framework based on international best practices. It was for this reason that the Electronic Communications and Transactions Act was enacted by Botswana in 2014 in order to give the country a foundation from which to start capitalising on the opportunities offered by e-commerce.

The Electronic Communications and Transactions Act thus facilitates and regulates digital communications and transactions (Government of Botswana 2014b). It recognises digital signatures and records emanating from e-mail communication. In essence, the legislation makes digital records admissible in legal proceedings as long as there is compliance with the provisions of the Electronic Records (Evidence) Act. Section 26 of this Act prescribes methods of accrediting products or services required for the authentication and recognition of secure digital signatures. The prescribed methods have to be consistent with international standards. A parastatal organisation, Botswana Communications Regulatory Authority, is responsible for the accreditation of certification service providers as well as the recognition of foreign certificates. Section 29 of the Act prescribes factors necessary for reliable and secure information systems and, in so doing, the following have to be considered:

a. Financial and human resources, including the existence of assets
b. Quality of hardware and software systems
c. Procedures for processing of certificates of digital signatures of service providers and the retention of records
d. Availability of information to signatories identified in certificates and to potential relying parties

e. Regularity and extent of audit by an independent body
f. The existence of a declaration by the Botswana Communications Regulatory Authority of the certification service provider regarding compliance requirements to be met for issuing digital signatures

2.2.6 National ICT Policy

Public sector agencies have increasingly relied on the use of computers as a means of creating, storing, managing and distributing their documents, reports and records (Parer 2000: 32). The Government of Botswana developed the National Information and Communication Technology Policy, popularly known as the Maitlamo Policy, to utilise the potential of ICTs to improve service delivery and to provide a national framework for the development of IT initiatives in the country (Government of Botswana 2007; Mosweu 2012:6; Moatlhodi 2015:43). Through the Maitlamo Policy (Government of Botswana 2007: 5), Botswana seeks to be a globally competitive, knowledge and information society where lasting improvement in social, economic and cultural development is achieved through the effective use of ICTs.

The National ICT Policy provides a general framework for using ICTs in public service delivery. By their nature, the use of ICTs generates digital records (Wamukoya & Mutula 2005a:67-68). However, the policy does not have specific guidance on how the resultant digital records from transactions done through ICTs should be managed. The policy provided for the formulation of a national e-government strategy for Botswana.

2.2.7 National E-Government Strategy

Through the national e-government strategy, the Government of Botswana seeks to use ICTs in public service delivery platforms to propel the transition of the country into a knowledge society; thus, assuring economic diversification and sustainable economic development (Government of Botswana 2012: 6). The e-government programme endeavours to move all appropriate government information online with focus on the following:

E-services programme (ESP): It is made up of 14 projects to be introduced in three (3) phases over the five-year period. The aim is to strengthen the portal as the primary service delivery vehicle for 300 identified government services. It includes the implementation of service delivery through mobile phones.

The Multiple Access Programme (MAP): The MAP will seek to deal with the fragmented projects by consolidating them into a consistent and effective approach to the provision of government information and services through multiple delivery channels. Projects earmarked are (a) introduction of central government contact centre, (b) introduction of government service centres countrywide, (c) integration and standardisation of e-government service delivery through CACs such as Kitsong and other access centres, (d) acceleration of the introduction of important e-government services directly through ministries.

Botswana's e-government, Service Transformation, Reform, Organisational and Network Governance (Be STRONG) Programme: This aspect will deal with the review and redesign of governance structure required to progress the national e-government programme. The role of government CIO will be considered to strengthen the project management office.

The Skills Transformation in Support of E-government Programme (STEP): A partnership between private and public training institutions will undertake a review of skills and training required in the public sector across all levels of officers in the government (Government of Botswana 2012:13-15).

The digital revolution, occasioned by e-government initiatives, has led to increased digital communication as well as the quantity of digital records created and maintained in digital formats (Nengomasha 2009:41; Luyombya 2010:51; Moatlhodi 2015:5). Such records need to be managed properly. Franks and Kunde (2006:55) observe that parallel to the increased volume of born and stored digital records, have been concerns over the ability to ensure that they continue to be accessible throughout their life cycle. Through the e-government strategy, the Government of Botswana is aware of resultant born and stored digital records from various computer information systems deployed as part of the e-government programme. Various pieces of legislation such as the Electronic Communications and Transactions Act and the Electronic Records (Evidence) Act were enacted while the Cybercrime and Computer Related Crimes Act (CCRCA) were amended to recognise digital records as evidence in court just like paper records (Keetshabe 2015). According to Nengomasha (2009:42), it is upon governments to ensure that record-keeping requirements are taken care of when deploying respective e-government systems and programmes. Such record-keeping requirements ensure the creation, capturing, maintenance of reliability and authenticity, sharing and preservation of digital records.

2.3 Maintaining the Authenticity of Records in Digital Systems

Transactions performed through digital information systems produce digital records. Pearce-Moses (2005:140) defines a digital information system as an automated system that facilitates access to and management of information and records in a computer system. Information systems are used to collect (or retrieve), process, store and distribute information to support decision-making and control in an organisation (Laudon & Laudon 2014:45). Information systems store data in discrete chunks that can be recombined and reused without reference to the documentary context, meaning that they are not necessarily record-keeping systems (South Carolina Department of Archives and History 2005:3). Comparatively, a record-keeping system has a set of rules governing the storage, use, maintenance and disposition of records and/ or information about records, and the tools and mechanisms used to implement these rules. Record-keeping systems are trusted information systems (InterPARES 2008).

2.3.1 Trusted Information Systems and Records Authenticity

The emergence of the concept of e-government around the 1990s throughout the world led to structural and process change in public administration, such as the increased deployment of different ICT platforms and applications for efficient and effective service delivery (Evans & Yen 2005; Wamukoya & Mutula 2005a; Sisman 2012). For example, in e-government, services such as acquiring and providing products as well as obtaining information or completing business transactions are expected to be done digitally (Fang 2002:13). According to Makhura (2005), in recent years, ICTs have positioned themselves as tools for the creation, access and retrieval of records. It is against this background that digital records generated from business systems need to be captured as authentic and reliable business records (South Carolina 2007:2). Trustworthy information systems are thus reliable, authentic and have integrity. Tafor (2003) and Stair and Reynolds (2006) caution that digital records are susceptible to easy manipulation even though they should remain available, usable, understandable and authentic for as long as needed.

The increased deployment of ICTs for providing records creators with the ability to create, store, modify, distribute and preserve digital records in a networked environment has posed a series of challenges for custodians who now have to keep new knowledge for maintaining such systems (Park 2001:270; Jansen 2014:39). The challenges are technical and administrative in nature. For example, the technological infrastructure for the acquisition and maintenance of resultant digital records need to ensure their authenticity in the long term (Jansen 2014:39).

The quest for maintaining the authenticity of records once created has a long history. Developed by Mabillion in the late 17th century, diplomatics was concerned with proving the authenticity and, indirectly, the reliability of archival documents for establishing the existence of patrimonial rights of the church, religious orders and other authorities. It was also used to identify and eliminate forgeries (Duranti 1997:213; MacNeil 1998: 107; Jantz 2009:73; Duranti 2014:5). Traditionally, diplomatics has been defined as “written testimony or evidence of a juridical fact, produced by a natural or juridical person in the course of practical-administrative activity, and kept for action or reference by that same person or its legitimate successor(s)” (Duranti 1997:214). Although the definition perfectly suited the purposes of diplomatics and archival science (for some time), it was found wanting for the research purposes of the University of British Columbia’s InterPARES when the research team tried to apply it to the digital records creation environment (Duranti 1997:214). Mak (2012:4) simply defines diplomatics as the systematic analysis of documentary evidence. It offers a method of interpretation founded on the intimate study of archival sources, including their material, form and the conditions of their production.

The concept of trustworthiness in classical diplomatics was equated with authenticity and implied a presumption of reliability, accuracy and legitimacy, and therefore genuineness (Rogers 2015a:21). It was possible to arrive at this inference due to the highly controlled process of creation, maintenance and preservation of ancient documents that were the subject of study of the early diplomatists. By establishing the identity of the document, its integrity was presumed. The advent of digital records meant this long-held view and reality ceased to hold truth. With digital records, identity and integrity are no longer linked (Duranti & Eastwood 1995:215). In the digital environment, much of a record's trustworthiness (which for the paper record was embedded within the document itself) is now located externally and must be verified through its provenance (Duranti 2010:81; Sullivan 2013:24). Instead, the components that make up what a record is, are stored and managed separately (Duranti 1997:217; Duranti 2010:81), as metadata (MacNeil 1998:117; Rogers 2015a:21).

In the digital environment, classical diplomatics became inadequate in the analysis of extrinsic and intrinsic elements of documents in the quest to establish their authenticity and reliability (Director 2005:4). For it to remain relevant in the view of records produced by 20th century bureaucracies, there was a need to apply diplomatics broadly and thus be redefined. As a result, the purpose of diplomatic analysis was required to be much wider than Mabillon's because of the need to:

- include informal documents as well as formal
- encompass aggregations of documents as well as individual ones
- consider the organisations and systems producing documents as well as the documents themselves
- enable prospective as well as retrospective analysis
- encompass digital as well as paper-based systems (Director 2005:4).

The redefinition of diplomatics by Duranti (1998) as “the discipline which studies the genesis, forms and transmission of archival documents, and their relationship with the facts represented in them and with their creator, in order to identify, evaluate, and communicate their true nature” appears to enable at least some of the broader applications articulated by Director (2005:4).

2.3.2 Characteristics of authentic records

Authentic records are authoritative (ISO 2016). According to Rogers (2015), authenticity of a record is reliant upon establishing and preserving the identity and the integrity of a record from its point of creation and thereafter. According to the IRMT (2009:2), the authenticity of a digital record derives from three essential characteristics of reliability, integrity and usability. From the assertions by the cited authorities it is clear that authentic records can be relied upon to support decision-making because they are reliable and have integrity. Their usability is without question because they are authoritative.

Authors such as Gibson (2001:65-66), Duranti (2001:44-48), InterPARES (2005) and Duranti (2010:83) assert that ensuring the authenticity of digital records in an information system entails undertaking the following:

a. Defining records’ access privileges.
b. Establishing routines according to which the digital system will generate a link between records.
c. Establishing procedures to prevent loss or corruption of records through intentional or inadvertent unauthorised additions, deletions or alterations.
d. Maintaining audit trails of transmissions and of access to the record system.
e. Establishing procedures for taking records out of the live system for preservation purposes.
f. Establishing records storage facilities and equipment requirements.
g. Establishing methods and rules for authentication.

h. Designing profiles, including fields that allow the verification of records identity and integrity.
i. Establishing procedures to prevent the loss of records due to factors such as technological obsolescence (of hardware, system software, and storage media such as: storage devices, access methods, and database management system).
j. Defining rules for moving digital records inside and outside of the organisation.
k. Compiling all the above policies and ensuring that every migration procedure that has occurred has been properly documented outside of the system.

- **Reliability**: The reliability of a record refers to the trustworthiness of a record as a statement of fact relating to the content. The assessment for reliability is based on the completeness of the record, that is, the presence of all the formal elements required by the juridical-administrative system for that specific record to be capable of achieving the purposes for which it was generated (Duranti 2009:52). The reliability of a record is its ability to serve as reliable evidence (International Council on Archives 1997:29). According to ISO (2016), a reliable record is the one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest.

As observed by Gibson (2001:65), InterPARES (2005) and Duranti (2010:82), the following measures are a necessity in order enhance the reliability of digital records in an information system:

a. Established body rules governing, making, receiving, routing, annotating and setting aside of records.
b. Predefined standard formats and templates.
c. Authenticating records using pre-established methods, depending on record type and function.
d. Embedding in the digital records system access privileges by assigning to each person who has access to the digital system, on the basis of clearly identified competencies,

the authority to compile, classify, annotate, read, retrieve, transfer, or destroy only specific groups of records.

e. Embedding in the digital records system "workflow rules" according to which the system will present only the person competent for each action with the related records and will solicit the making of the appropriate record at the proper time in the automatic development of the procedure.
f. Limiting access to the technology or to parts of it by means of magnetic cards, passwords and fingerprints.
g. Designing within the digital system an audit trail, so that any access to the system and its consequences (e.g. a modification to the record, a deletion, an addition) can be documented as they occur.

- **Integrity**: Integrity is one of the features of an authoritative record. A record possesses some integrity if it is complete and unaltered ISO (2016). A record should be protected against unauthorised alteration. Policies and procedures for managing records specify the additions or annotations made to a record after it is created, including the rules governing the circumstances under which such additions or annotations can be made and authorised. This also includes the person who has authorised their addition. According to InterPARES (2002), the integrity of a record refers to its wholeness and soundness: a record has integrity when it is complete and uncorrupted in all its essential respects. Of notable importance is that a record that possesses the characteristic of integrity does not need to be exactly the same as it was when first created for its integrity to exist and be demonstrated. Records in both the digital and paper world are subject to deterioration, alteration and/or loss. In the digital world, the fragility of the media, the obsolescence of technology and the idiosyncrasies of systems likewise affect the integrity of records (InterPARES 2002).

  For records integrity to be maintained, organisations should follow IT profession best practices for data preservation. Systems must ensure the following (Library of Virginia 2009:6):

a. A record creator's identity is verified.
b. Restrictions exist regarding permissions to read and write files.
c. Periodic system audits are conducted.
d. Data transmission includes data error checking and correction.
e. Data backup occurs regularly.
f. Data on off-line media are regularly refreshed to avoid loss of data due to degradation.

- **Usability**: A useable record is one that can be located, retrieved, presented and interpreted within a time period deemed reasonable by stakeholders (University of Tasmania 2014; ISO 2016). Useable records do not exist in isolation. They are related to others and this linkage comes from connected business processes or transactions that produce them (ISO 2016). According to the Government of Hong Kong (2011:5), records have usability when they are connected to the business activity or transaction that produced them. The record has to be retrievable, presentable and the data therein have to be correct (Mason 2007:36).

- **Identity:** The maintenance of the identity of a record, together with its integrity, ensures that digital records are authentic over their life cycle (MacNeil 2000b:53; Tennis 2012:38; Rogers &Tennis 2013:801). The authenticity of a record is assessed in relation to its identity (i.e. was it written by the person who purports to have written it?) and its integrity (i.e. has it been altered in any way since it was first created and, if so, has such alteration changed its essential character?). According to Park (2005:9), digital records are vulnerable and susceptible to alteration and therefore their authenticity needs to be maintained. In the digital environment, maintenance of records authenticity is more difficult because the identity of a record is not linked to its integrity (Duranti & Eastwood 1995:215). The trustworthiness of a record is located externally and must be verified through its provenance (Duranti 2010:81; Sullivan 2013:24), thus the components that make up a record are stored and managed separately (Duranti 1997:217; Duranti 2010:81) as metadata (MacNeil 1998:117; Rogers 2015a:21).

2.3.3 Criteria for Assessing Authenticity of Digital Records

Ensuring the authenticity of records entails an analysis of the components of an archival document (MacNeil 2000a:96). According to MacNeil (2000a:96), based on diplomatic analysis, "electronic records possess essentially the same components as traditional records", although not inextricably joined to one another as is the case in traditional records. Instead, they are stored and managed separately as metadata of the digital system and metadata of the records (MacNeil 2000a). These scholars (MacNeil 2000a: 91-95; Duranti 2001: 272-273; Duranti, Eastwood & MacNeil 2002: 12-20) indicate that in the digital environment, external and internal elements that constitute a digital record include the following metadata elements:

a. Medium; the physical carrier of the message.
b. Content; the message intended to be conveyed by the record.
c. Physical form; the formal attributes of the record that determine its external make-up (e.g. script, type font, special signs, seals of any kind, colours, language, inserts, format and script.
d. Intellectual form; the sum of the record's formal attributes that represent and communicate the elements of the action in which the record is involved and of its documentary and administrative contexts.
e. Context; the juridical, administrative, procedural and documentary framework in which the record is created.
f. Archival bond; the relationship linking each record to the previous and subsequent one and all others participating in the same activity.
g. Persons; the entities acting by means of the record.
h. Action; the exercise of will that gives origin to the record.

2.3.3.1 Specific methods for ensuring authenticity of digital records

The authenticity of digital records is linked to the record's mode, form and state of transmission, the manner of preservation and custody (MacNeil 2000a). Authenticity is protected by instituting methods that ensure that a record is not manipulated, altered or falsified after creation and that it remains reliable as it was when first created. Therefore, authentic records are transmitted securely when their state of transmission can be ascertained and preserved in a secure manner and its provenance can be verified (MacNeil 2000a). Examples of such methods include encryption of records, maintaining of an audit trail of a record's transmission, appending of digital signatures to records and establishing of the status of transmission of records (MacNeil 2000a).

Szívós and Orosz (2014:162) note that information technology-based information systems such as Enterprise Resource Planning systems are now common in businesses. They provide a platform where master data and master files of financial data are managed and maintained. Transactions that increase the risk of misstatements such as data migration or unauthorised change of data in master files are a reality. These can have an adverse impact on the level of risk perceived by auditors who have to maintain the overall audit risk at an acceptable level. Szívós and Orosz (2014:162) add that the accuracy and relevance of master data and master files are crucial as it is through them that a fair presentation of financial statements can be realised.

Records in in the digital environment are prone to accidental or deliberate alteration because of evolving digital technologies (State Comptroller of Israel 2004:16; Duranti & Blanchette 2004; Boudrez 2005:1; Xie 2011:577). Therefore, maintaining the authenticity of such records entails that the presumption of that authenticity must be supported by evidence of it by way of establishing their identity and demonstrating their integrity (Duranti & Blanchette 2004; Mason 2007:32). One way of doing that is to authenticate digital records in the system (McDaniel 2006:4; Mason 2007:32). Through authentication, an individual's identity as a party to the transaction is confirmed (Tank, Emley & Whitaker 2013:28). Authentication of identity in digital transactions occurs initially when the transaction first takes place and when it recurs during the course of undertaking business transactions.

A number of technologies and methods are used to establish the authenticity of digital records and users. These include digital signatures, timestamps, hash digests, passwords, randomly generated numbers, biometric measurements, checksums and cyclic redundancy checks (Elliot 2007:2; Mir & Banday 2012:225; Tank et al. 2013; Turkish Standards Institution 2014:12). These technologies control access to digital systems (Tank et al. 2013). The environment dictates the choice of technology to be deployed (Elliot 2007:2).

2.3.3.2 Specific methods for ensuring reliability of digital records

The reliability of a record, meaning its capacity to stand for the facts to which it attests, is "associated with the creation of a record and refers to the completeness of its intellectual form and the degree of control exercised over its creation procedures" (MacNeil 2000a:100). The reliability of a record created by using information and communication technologies makes it difficult to conclude that it is complete, let alone for anyone to assume that it is sufficiently reliable (Lee 2005:1). Elements of a digital record should be present for a digital record to be capable of generating consequences. Such elements include date of record, time and place of creation, transmission and receipt, identification of names of author, addressee, originator and writer (if both are different from the author), name of creator, title or subject line, classification code and any other element required by the creator's procedures and juridical system (MacNeil 2000a). The procedures or body of rules relating to the record's creation determines its reliability. Such body of rules governs the making, receiving and setting aside of records and it refers to establishing who is competent to create, modify and annotate records, and how records should be routed and filed. Duranti (1995) opines that the more rigorous the rules, the more reliable the records will be. According to MacNeil (2000a), respecting these rules through a preventative and verification regime ensures the reliability of records.

2.3.4 Empirical Studies on Authenticity and Reliability of Digital Records

For three decades prior to 1997, archivists and records managers worked hard to cope with continuous changes inherent in digital information systems containing records (Cox 1997).

This meant that system designers, high-technology companies and information policymakers, among others, produced volatile solutions and digital information infrastructure that could render obsolete solutions thought to be viable only a few years before. The endeavour to produce reliable systems that produced and managed digital records resulted in several empirical studies. These included the University of Pittsburgh, the Preservation of the Integrity of Electronic Records: UBC – MAS Project and the International Research on Permanent Authentic Records in Electronic Systems (InterPARES) (Duranti & MacNeil 1996; Cox 1997; Bearman & Sochats 2004).

2.3.4.1 The University of Pittsburgh Project

The University of Pittsburgh Project, which set out to develop functional requirements for record keeping in digital environments, was jointly led by Professor James Williams and Professor Richard J Cox of the University of Pittsburgh's School of Information Sciences following a research grant of $359,560 received from the National Historical Publications and Records Commission in 1993 (Cox 1997). According to Duff (1996) and Rogers (2015b:32), the project focused on recorded transactions providing evidence. Undertaken over three years, the project produced a set of 19 functional requirements for digital evidence based on literary warrant (Rogers 2015b:32). Rogers (2015) avers that although the project did not specifically address records authenticity explicitly, it produced requirements supported by trustworthiness and accountability. However, the record-keeping functional requirements were observable and measurable to the extent that software engineers could use them to develop systems that incorporated the requirements and made it possible for records as defined by the requirements to be maintained in such systems.

2.3.4.2 The preservation of the integrity of electronic records (UBC-MAS Project)

The origins of the Preservation of the Integrity of Electronic Records (UBC-MAS Project) mirror those of the University of Pittsburgh Project. According to Marsden (1997:159), "the inescapable and well documented requirement for theoretical and practicable models to confront the intersection of technology and the management of records and information” led to the birth of the project. Specifically, the project set out to define the methods for ensuring reliability and authenticity of digital records based on diplomatic and archival concepts and principles. Duranti and MacNeil (1997) point out that the UBC Project studied the authenticity and reliability of digital records from the point of view of the records creator, specifically a corporate body. This was because corporate bodies depended on making and maintaining records that had integrity when undertaking their activities.

The specific objectives of the project were to:

- establish what a record is in principle and how it can be recognised in the digital environment
- determine what kind of digital systems generate records
- formulate criteria that allow for the appropriate segregation of records from all other types of information in digital systems generating and/or storing a variety of data aggregations
- define the conceptual requirements for guaranteeing the reliability and authenticity of records in digital systems
- articulate the administrative, procedural and technical methods for the implementation of those requirements; assess those methods against different administrative, juridical, cultural and disciplinary points of view (Duranti & Eastwood 1995:215; Duranti & MacNeil 1997:47).

Firstly, the UBC-MAS project defined the terms ‘reliability’ and ‘authenticity’, which, when combined, amount to integrity (Duranti 1995). Rogers (2015) opines that preserving the integrity of records means ensuring that they are created reliably and maintained authentically. The meaning of the concepts of reliability and authenticity were derived from diplomatics (Rogers 2015b:21). Reliability refers to the authority and trustworthiness of records as proof and memory of the activity, including their ability to stand for the facts they are about. Authenticity is defined as the trustworthiness of a record as a record, that it is what it purports to be and is free from tampering or corruption (Duranti 2001a).

The UBC research team collaborated with the US Department of Defence Records Management Task Force and operationalised the research findings in the form of mandatory functional requirements for records management application software (DOD 5015.2 STD) (Duranti, MacNeil & Underwood 1996; MacNeil 2000a). Through the collaborative research agenda, the two partners sought to interpret archival and diplomatic concepts using a standard modelling technique (**I**ntegrated **DEF**inition language) (Duranti, Eastwood & MacNeil 2003). According to Duranti and MacNeil (1997:64), the results of the tests of validity of traditional archival and diplomatic concepts were found to provide a “powerful and internally consistent methodology for preserving the integrity of digital records” (Duranti & MacNeil 1997:64).

2.3.4.3 International research on permanent authentic records in electronic systems

Another project that studied the management of records in the digital environment is commonly known as International Research on Permanent Authentic Records in Electronic Systems (InterPARES) (Duranti 2009). Based at the University of British Columbia, InterPARES is the longest running and longest continuously funded research project into the preservation of authentic digital records (Rogers 2015b:37). In the words of Duranti (2009:3006), “InterPARES has developed knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form, and provided the basis for standards, policies, strategies and plans of action capable of ensuring the longevity of such material and the ability of its users to trust its authenticity.”

InterPARES I Project (1999-2001) focused on the preservation of the authenticity of digital records no longer required for operational and business purposes (InterPARES 2005). The records examined were primarily textual documents produced and maintained in databases and document management systems. According to Rogers (2015b:38), the concepts of reliability, authenticity, record and digital record adopted and developed by the previous UBC Project formed the basis of inquiry. InterPARES 1 had its epistemological roots in the humanities, specifically in diplomatics and archival science (Duranti 2007). It sought to establish the means for assessing and maintaining the authenticity of digital records once they become inactive and are selected for permanent preservation (InterPARES 2005). Research teams were drawn from across the whole globe and came from disciplines such as law, history, computer science and engineering, information science, and chemistry. However, the project's key concepts and methodologies were drawn from diplomatics and archival science (InterPARES 2005). InterPARES 1 comprised taskforces, one of which was the Authenticity Task Force. The Authenticity Task Force developed benchmark requirements that supported the presumption of the authenticity of digital records before they are transferred to the preserver's custody and those that supported the production of authentic copies of digital records after they have been transferred to the preserver's custody (Duranti 2001b; InterPARES 2005; Rogers 2015b:40).

InterPARES 2 Project (1999-2001) built upon the findings of InterPARES 1 and sought to address the challenge of the permanent preservation of reliable, accurate and authentic digital records created and maintained in interactive and dynamic systems in the course of all kinds of human activities (Duranti 2007; InterPARES 2008). Being archival in nature, the ultimate goal of InterPARES 2 was the development of a trusted record-making and record-keeping system and of a preservation system capable of ensuring the authenticity of the records under examination over the long term (Duranti 2007). Thus, the work carried out throughout the project in the various disciplinary areas had to be constantly translated into archival terms and linked to archival concepts, which are the foundation upon which the systems intended to protect the records. In terms of research methodology, InterPARES adopted no epistemological perspective. According to InterPARES (2008), the second InterPARES project probed the issues of reliability and accuracy during the entire lifecycle of records, from creation to permanent preservation. Domains that drove the project focused on (1) digital records creation and maintenance, (2) authenticity, reliability, and accuracy of digital records in the artistic, scientific and governmental sectors and methods of appraisal and preservation.

Among its key products, InterPARES 2 produced a set of guidelines for creators and preservers that operationalised the Benchmark and Baseline Requirements that emanated from InterPARES 1 and was a further development of it (Roeder, Eppard, Underwood & Lauriault

2008). This was developed with input from archival scholars, practicing archivists and specialists in the arts, sciences and government. Roeder et al. (2008) acknowledge the usefulness of the guidelines in informing the preservation of digital records, but pointed out that they should not be used blindly as they have not exhausted all preservation-related issues. Despite this cautionary measure, Rogers (2015b:47) notes that the guidelines are still highly referenced and used, as evidenced by the frequency of downloaded resources from the InterPARES website. The other products of InterPARES 2 were a framework of principles guiding the development of policies for records-creating and -preserving organisations; guidelines for making and maintaining digital records for individuals and small communities of practice; guidelines for digital preservation for archival institutions; a metadata registry for the registration and analysis of metadata schemas; a chain of preservation model; principles and criteria for the adoption of file formats, wrappers and encoding; and a terminology database (Duranti 2007; Roeder et al. 2008).

InterPARES 3 took place from 2007 to 2012. It built upon the findings of InterPARES 1 and 2 and other digital preservation projects worldwide (Rogers 2015). It used findings from previous InterPARES projects and other research projects to put theoretical concepts into practice by applying research findings of the previous two phases through case studies with small- and medium-sized organisations, or those with limited resources. For example, Rogers, Daum, Shaffer and Allen (2013) undertook a study to develop a policy and procedures for the preservation of digital records at the British Columbia Institute of Technology (BCIT). This case study followed the general case study methodology determined by InterPARES. Data collected from standardised InterPARES questionnaires and interview protocols were measured against the InterPARES Benchmark and Baseline requirements for the creation and preservation of authentic reliable records to conduct a gap analysis in order to determine deficiencies in current practice. At the end, Rogers et al. (2013) indicate that a policy and records management procedures for digital records were developed using the InterPARES framework of principles for the development of policies. This included strategies and standards for the long-term preservation of digital records as a guide for content that reflected best practice, and existing BCIT records management policy and procedures as a guide for form.

InterPARES 4 (2013-2018) was known as InterPARES Trust. It studied issues of trust in records maintained and used in online environments (Rogers 2015b). According to the InterPARES Trust website at https://interparestrust.org/, the InterPARES Trust research project comprises multidisciplinary teams across the globe. The focus of research is on exploring issues concerning digital records and data entrusted to the internet. The main goal is to come up with theoretical and methodological frameworks applicable for developing local, national and international policies, procedures, regulations, standards and legislation that can assist in ensuring public trust grounded on evidence of good governance, a strong digital economy and a persistent digital memory.

Goh (2014) illustrates how records-related archival legislation was left behind by technology in a study that analysed court cases related to audio-visual materials from Canada, Singapore and Australia. The audio-visual material created in a cloud environment was analysed. Issues about applicability of national laws over the control, ownership and custody of data and records were explored. The study concluded that current records and archival legislation does not address issues related to the creation, processing and preservation of records and data in the cloud.

In a related study, Ngoepe and Saurombe (2016) analysed archival legislation in nine member countries of the SADC for the provision of management and preservation of records created in networked environments. The study revealed that only South African legislation has specific provisions for digital records management while others were silent. Furthermore, the study revealed that there was lack of archival legislation that recognised digital records from digital transactions as admissible evidence by the courts. That provision was found in digital communications and evidence acts of Botswana, South Africa, Swaziland and Tanzania. Except for legislation in South Africa, archival legislation did not specifically define digital records, but included them in the broader definition of a record. Inadequate archival legislation for the management of digital records was also revealed by a comparative study on the state of national archival and records systems between South Africa and Botswana (Ngoepe & Keakopa 2011) and another one, which investigated the role of a computerised court records system in the delivery of justice in the Magistracy in Botswana (Mosweu 2012). Consequently, the study by Ngoepe and Saurombe (2016:38) recommended that the SADC should consider adding a legal instrument in the form of a protocol on archival legislation that would pave the way for the development of a localised statute on the management and preservation of digital records.

Bhebhe (2015:107) sought to find out how the originality, authenticity, reliability and genuineness of legal records found at the National Archives of Zimbabwe were maintained with a focus on provenance issues and implications diplomatics. Collecting data through observation and document analysis, the study found that the national digital heritage of Zimbabwe was being lost due to archaic archival legislation that was silent on digital records. It was also found that although the Zimbabwean government produced both digital and paper records, the National Archives of Zimbabwe only archived paper records, the result of which is incompleteness of records, which negatively affected their diplomatics.

An ongoing study by Katuu and Ngoepe (2015a), as part of the InterPARES Trust Team Africa, focuses on "*Curriculum Alignments at Institutions of Higher Learning in Africa: Preparing Professionals to Manage Records Created in Networked Environments.*" The study sought to systematically analyse the curricula of educational institutions offering archives and records management education and training across Africa in order to ascertain the extent to which the curriculum addresses the education and training needs of archives and records management professionals in a networked environment. The study was conducted in the following phases:

a. The first phase reviewed literature examining the use of published sources to gauge what has taken place both within individual countries and on a regional or even continent-wide basis. An annotated bibliography has been completed (InterPARES 2016b).
b. The second phase sought to produce an inventory of all possible programmes that offer formal opportunities for archives and records professionals' education and training. This phase is ongoing.

c. The third phase entailed the assessment of curricula of selected institutions representing different regional or programmatic flavours. The assessment will be looking at the extent to which the curricula address modern challenges.

d. The fourth phase was a tracer study of selected graduates from programmes in order to assess the extent to which their working environment reflects their educational and training background (Katuu & Ngoepe (2015a:6; InterPARES 2016b). All the phases were scheduled to take place between 2015 and 2018.

Katuu and Ngoepe (2015b:59) studied the management of digital records within South Africa's legislative and regulatory framework. The study realised that technological developments have brought with them challenges that are a hindrance to the effective management of digital records in the context of South Africa. Already grappling with the emergence of the impact of personal computing which decentralised records creation and management (McDonald 1995), a greater challenge emerged with the issue of cloud computing, a model "for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (McClelland et al., 2014). Duranti (2013:51) specifies the challenges encountered by records management professionals in managing records in the cloud. These relate to the need to address issues of jurisdiction, control, custody and trust. In the context of South Africa, the question is whether the legislative and regulatory framework is adequate to facilitate the management of digital records in public institutions.

Despite South Africa having legislation that covers the management of digital records such as the Electronic Communications and Transactions (ECT) Act, enacted in 2002 to facilitate digital communications and transactions by promoting legal certainty whenever public administration and private business activities need to be conducted in digital form (Government of South Africa 2002a:16-18), and the Regulation of Interception of Communications Act (RICA), also enacted in 2002 to regulate the interception of certain telephonic as well as internet communication (Government of South Africa 2002b). The two authors, Katuu and

Ngoepe (2015b:4-5), note the following challenges that relate to the management of digital records.

a. The first challenge relates to the weaknesses presumed as the functional equivalence between digital and hard copy records (Xie 2011:6). In a hard-copy environment, a record has stable content existing in a fixed documentary form. In the digital environment, a digital record's documentary form "may neither be fixed nor stable in the traditional sense" and the intrinsic and extrinsic elements of form are not necessarily dependent on, nor inextricably linked to, a physical medium (Rogers 2015:8). This makes the documentary form of digital content in complex information systems such as relational databases and systems (with different layers of content such as geographic information systems) more difficult to determine. This is the reason why Thibodeau (2012:16) concludes that defining digital records and simultaneously trying to isolate their boundaries, is a difficult task.

b. The second one is about differentiating between an original digital record and its copy (Katuu & Ngoepe 2015b:5). According to Force (2013:127-128), judges in courts sometimes base their decision to admit copies as evidence on whether counsel could explain why an original could not be produced. Accordingly, this situation suggests that the records manager should be able to facilitate the location of the original and/ or copy of the record. This can be done by using an approved records retention and disposal schedule, which could shed light on the destruction of records and counsel can use that information to explain to the judge why particular records or their versions are not available.

According to Duranti and Blanchette (2004:4), traditionally, preservers were mandated to issue copies and attest that they conformed to the original being reproduced and were thus authentic. In the digital environment, this is made difficult by issues related to records preservation and the ability to maintain documentation of the activity of reproduction to support its attestation of authenticity. Authentic copies can be deemed as such if attested to be so by the official preserver and if such attestation is supported by the preserver’s ability to demonstrate that all the requirements for the production of authentic copies have been satisfied (Duranti & Blanchette 2004:4). Attested this way, the copy is deemed to conform to the record it reproduces until proof to the contrary is given.

Apart from the aforementioned, metadata can be used to account for who may have destroyed the record or its version and when (Force 2013:127-128). To this end, Katuu and Ngoepe (2015b:5) suggest that, over and above the call by the South African Law Reform Commission (2010:52-53) to review the definition of data message and the inclusion of digital, ‘copy’ and ‘original’ in the ECT Act (Government of Botswana 2014b), they further call for an examination of the law of evidence, inclusive of other legislative instruments as well as an exploration of the implications on the record-keeping practices in the country’s public institutions, as that is critical when dealing with digital evidence of transactions and communication in South African legal proceedings (Mostert 2005:7).

2.4 Capabilities and Competencies Required for Judging Authenticity of Digital Records

Audit professionals, apart from those who qualify to be accountants, need to take educational courses so that they can acquire the requisite capabilities required in modern-day auditing (International Federation of Accountants 2005:11). These courses can be done simultaneously with those needed to qualify as accountants or thereafter and may include on-the-job training and experience programmes, off-the-job training and continuing professional development (CPD) courses and activities (International Federation of Accountants 2005:11). The International Federation of Accountants indicates that auditors performing audits in a digital environment should possess knowledge content, which include IT systems for financial accounting and reporting (including relevant current issues and developments), principles and practices for evaluating financial accounting and reporting systems (including evaluating controls and assessing risk) and computer-assisted auditing packages and techniques. According to Carroll (2006:63), auditing in a digital environment entails that auditors should select, gather, analyse and report, and thus help in adding credibility to audit findings, conclusions and recommendations. For example, they can use audit tools and techniques such as Generalised Audit Software (e.g. ACL, IDEA, Microsoft Excel or SQL queries).

Records managers and ICT specialists also need to have the required competencies and skills to manage records in the digital age. Recognising that the digital age requires a skilled and knowledgeable workforce with capabilities needed for ensuring that digital information remains accessible and usable over time, the National Archives of Australia (2015:2) developed a digital information and records management capability matrix for records managers and ICT specialists to enable them to cope with requirements for the management of digital records (National Archives of Australia 2015:3-10).

The National Archives of Australia is an agency responsible for advising all Australian government agencies on ways of improving digital information management for business efficiency and effectiveness and to ensure transparency and accountability (National Archives of Australia 2015). This was in recognition that a skilled and knowledgeable workforce is crucial in managing digital information. The matrix presents the capabilities that agencies need for a changeover to a digital information management regime, which would make sure that information remains accessible and usable through the passage of time in the digital environment (National Archives of Australia 2015). It outlines generic capabilities for all staff, ICT and information and records management specialists. These capabilities, adopted as constructs, are used in this study to evaluate competencies and skills for records management and ICT professionals in relation to their ability to manage authentic digital records. These are presented at Table 2.1.

Table 2.1: Capabilities and skills of ICT specialists and records management personnel (National Archives of Australia 2015)

ICT specialists	Records management specialists
Awareness of legislation, standards and policies affecting information management	Awareness of legislation, standards and policies affecting information management

Metadata	Information governance and business risk mitigation
Information risks and destruction	Metadata
Interoperability	Risks to information
Technologies and tools	Retention and destruction of information
Data architecture	Access to information
User experience	Standards and best practices
Technologies and tools	Specialist technologies
Information costs	Communication and leadership
	User experience

The cited capabilities for records management professionals and ICT professionals clearly show that the capabilities required for managing records in the digital environment were influenced by the Australian tradition of the use of the Records Continuum Model (RCM). The model has been adopted to guide records management practice in Australia. The impact of computer technology on record keeping brought the reality that for digital data, the records life cycle model of records management was no longer applicable in an environment similar to the digital environment because the stages in the life cycle cannot be separated as the nature and volatility of the recorded data do not permit it (Atherton 1985: 47). For example, in the continuum model of records management, records creation as viewed in the life cycle approach is an ongoing process rather than an event in time (McKemmish 1998). Thus, a split between the records management and archival phases of the "life cycle" was no longer acceptable. Xiaomi (2003:25) notes that it was this kind of thinking that propelled the search for some sort of continuity between archives and records management.

The RCM as a concept to inform record keeping was formulated in the 1990s by Australian archival theorist Frank Upward based on four principles (Xiaomi 2003: 25).

1. A concept of record inclusive of records of continuing value (archives) stresses their uses for transactional, evidentiary, and memory purposes, and unifies approaches to archiving/record keeping, whether records are kept for a split second or a millennium.

2. There is a focus on records as logical rather than physical entities, regardless of whether they are in paper or digital form.
3. Institutionalisation of the record keeping profession’s role requires a particular emphasis on the need to integrate record keeping into business and societal processes and purposes.
4. Archival science is the foundation for organising knowledge about record keeping. Such knowledge is revisable but can be structured and explored in terms of the operation of principles for action in the past, the present, and the future

The RCM is viewed as better placed to guide the management of both paper and digital records (Ndenje-Sichalwe 2010: 58). It was a direct response to the capabilities of the Records Life Cycle Model (RLM) to influence the management of digital records (Shepherd & Yeo 2003: 9). The RCM is regarded as capable of providing a consistent and coherent regime of management processes from the time of creation of records and (before creation, in the design of record keeping systems) through to the preservation and use of records as archives (Flynn 2001:80). Upward (2001) holds the view that as a metaphor, the RCM can assist Australians to get records management ‘right’ in record keeping environments built around digital communications.

2.4.1 Computer Assisted Audit Techniques

Changes in the business environment have led to the implementation of new innovations for the accomplishment and advancement of organisations’ functions, one of which is information technology, which has made tools available for organisations to effectively and efficiently do their business (Rezaei 2013:90). Therefore, the benefits of computerising audit activities are undeniable (Kanellou & Spathis 2009:174; ACCA 2011:4; Moorthy et al. 2011:3523; Rezaei 2013:90). According to Elefterie and Badea (2016), the increasingly complex computerised accounting systems and the high volume of transactions recorded have seen an accelerated trend with a preference for computer assisted audit techniques (CAATs) over standard audit techniques.

Moorthy et al. (2011: 3523-3524) indicate that as part of the recognition of conducting audits in new IT environments, auditors must recognise reasons for the use of audit tools and software and such reasons, including the following:

(i) At a personal level, to learn a new skill.

(ii) To improve company decision-making using improved data.

(iii) An increase in the efficiency of an audit.

(iv) A reduction in routine tasks to provide more time for creative and business analysis.

(v) Improved transparency governance of the organisation.

(vi) Identification of quantitative root causes for issues.

(vii) Reduction in fraud and abuse.

(viii) Savings in supplier, customer, human resource, computer, and enterprise management.

The decision whether to use CAATs or manual processes in financial audit procedures stems from deliberate decisions based on a number of factors. ACCA (2011:4) lists them as the following:

(i) Practicality of carrying out tests manually

(ii) Costs involved in using CAATs

(iii) The time available to conduct an audit

(iv) Availability of the audit client’s computer facility

(v) Level of audit experience and expertise in using a specified CAAT

(vi) Level of CAATs carried out by the audit client’s internal audit function and the extent to which the external auditor can rely on this work

It would seem that for CAATs to be used as an audit tool, many factors come into play. The reasons advanced for utilising CAATs in audits suggest that, in totality, using CAATs rests on sound factors supporting usage and this goes beyond CAATs being a complex tool that are technical by nature.

Moorthy et al. (2011:3524) conclude that whether an organisation employs CAATs or uses manual processes for financial auditing, the objectives of accounting control remain the same. What differ are the procedures employed in the examination of financial statements. In that regard, SAS No. 48 recommends that auditors should evaluate the methods of computer data processing and other significant factors such as “planning and supervision, study and evaluation of internal control, evidential matter, analytical review procedures, and qualifications of the audit team” (Moorthy et al. 2011:3524).

2.5 Management of Authentic Reliable Records in Information Systems

Digital records need to be stored properly with access to them controlled in an appropriate and stable storage environment in order to be protected from alteration and corruption from the environment (National Electronic Commerce Coordinating Council 2004:12). In addition, for them to remain reliable and authentic, with their integrity maintained and useable as they are needed, their content and context, and sometimes structure, need to be preserved. The National Electronic Commerce Coordinating Council (2004:11) cautions that if the structure of a record is not preserved, its structural integrity is impaired, which in turn undermines the authenticity and reliability of the record. The National Information Standards Organisation (NISO 2004:1) advocates for the preservation of metadata of a record once it is created, to aid records storage and retrieval. The management and preservation of records in a digital environment are problematic due to a lack of storage and preservation measures in many countries. They are also more vulnerable than their paper counterparts and must be carefully managed to ensure their accuracy and authenticity as proof of accountability (Duranti 2001:275; Keakopa 2007:33; Luyombya 2010:59).

2.5.1 Metadata and The Management of Authentic Digital Records

Metadata is crucial in the management of records. Minnesota State Archives (2012:40) defines it as “data about data” and argues that it enables users of digital records to locate and evaluate data without each person having to discover it again with every use. Kalusopa (2011:5) defines it as background information required to make sense of a record. According to the IRMT (2008:6-8), making sense of a record requires that its content should be linked to its structure and context. Metadata is associated either with an information system or an information object for purposes of description, administration, legal requirements, technical functionality, use and usage and preservation (InterPARES 2008:1). It plays a crucial role in ensuring the creation, management, preservation, discovery, use and re-use of trustworthy materials, including records.

The IRMT (2008) identifies categories of recordkeeping metadata as structural metadata, which consists of information about the design of the data or records; contextual metadata which identifies the provenance of a record, such as the person or system responsible for creating it; and content metadata which contains the actual data that documents the transactions. According to InterPARES (2008:1), recordkeeping metadata plays a significant role in documenting the reliability and authenticity of records and record-keeping systems, including the various contexts (legal-administrative, provenancial, procedural, documentary and technical) within which records are created and kept as they move across space and time. The same record-keeping metadata makes it possible to identify, manage, store, use and reassemble record components to generate an authentic copy of a record (InterPARES 2008:1). Franks and Kunde (2006:56) hold the view that in modern-day information management, metadata must also be defined and understood in terms of the function it performs so that it is appreciated not only for what it is, but also for how it operates.

According to Minnesota State Archives (2012:42), metadata comprises basic elements of a structured format and a controlled vocabulary, which, together, allow for a precise and comprehensible description of content, location and value. Reed (2005:2930) says that recordkeeping metadata is of key importance in managing records in the digital world, because it is through the presence of metadata that particular resources can act as authoritative evidence of business actions. This involves records being sustainable over application system boundaries in ways that render them usable and interpretable for as long as they are required. Franks and

Kunde (2006:57) indicate that metadata facilitates interoperability across systems. The two scholars articulate the centrality of metadata in record keeping in a digital environment succinctly and Kunde (2006:61) who points out that metadata serves as the backbone of digital records management systems by providing consistent identification of records, preserving their authenticity and implementing retention and disposition requirements. Regarding the issue of long preservation of digital records, it plays a vital role in identifying key information necessary for conducting the conversion or migration processes, such as hardware and software used to create the digital information object.

NISO (2004:1) and IRMT (2008:66) identify three main types of metadata. These are descriptive metadata, which describes a resource for purposes of discovery and identification; structural metadata, which indicates digital objects put together; and administrative metadata, which provides information to help manage a resource, such as when and how it was created, file type and other technical information, and who can have access to it. Preservation metadata, which is a subset of administrative metadata but is sometimes categorised as another type of metadata contains information needed to archive and preserve an information resource (NISO 2004:1). Metadata is pivotal in ensuring that resources will survive and continue to be accessible in the future.

Appropriate and good records storage ensure that records are usable, reliable and authentic, and remain preserved for as long as they are needed (Kalusopa 2011:187). The international records management standard, ISO 15489-1, requires that “records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed” (ISO 2001:14). This is because there is a need for the storage of records throughout their life cycle to support business transactions, including digital records created through information systems (National Electronic Commerce Coordinating Council 2004:11). Unlike paper records that were managed long after creation, like being transferred to a records centre, digital records entail that, from the beginning, their management must be included in system planning and implementation as an organisation classifies its information for further use. This classification is vital for the application of corresponding digital controls to ensure the effective maintenance and disposition of the record.

Keakopa (2009:80-84), Kemoni (2009:192-195), Nengomasha (2013:5-7) and Marutha and Ngulube (2012:47-52) reveal a number of challenges related to the management of digital records in the ESARBICA region, including Botswana. This includes unstable digital media which become obsolete quickly; dependence on digital technology for the creation and storage, which means that they have to be managed in a computerised environment; deterioration of digital data over time, especially when not compliant with generic document standards such as Extensible Markup Language (XML) and Standard Generalized Markup Language (SGML). This deterioration reduces the quality and integrity of the digital records. Other challenges are outdated archival legislation which does not cater for the management of digital records; lack of policies, standards, procedures and guidelines for managing digital records (including their appraisal and disposition); lack of knowledge, competencies and skills for the management of digital records; inadequate infrastructure and poor management of official email records (Ngulube 2004; Mnjama & Wamukoya 2007; Keakopa 2008; Ngoepe & Keakopa 2011; Nengomasha 2013:3-7; Ngoepe & Saurombe 2016).

2.5.2 Disposal of Digital Records

Records disposal is an integral part of records management. When done properly, it ensures that records are retained for as long as they are needed and when they have surpassed their usefulness, they are either destroyed in an appropriate manner or transferred to an archives service (IRMT 2009:33; National Archives of UK 2011:3). According to the IRMT (2009:33) and the Government of South Australia (2014:6), preserving only valuable records while destroying obsolete ones ensures that only valuable records are retained, saving an organisation time and money. Unlike paper records, which can survive for long periods, digital records have a much shorter life span (IRMT 2009:33). This makes the disposal of digital records a necessary undertaking if they are to serve the needs of the organisation.

2.6 Summary

This chapter has reviewed literature related to the authentication of digital records in information systems in support of audit processes. In general, the practice of auditing of accounts was put into perspective as it relates to the centrality of records in the audit process. Specifically, issues of the authentic digital records were identified and discussed, particularly with auditing now being undertaken in the digital environment, due to the introduction of digital accounting systems. Criteria for the creation and maintenance of authentic digital records were ascertained. Furthermore, the capabilities and competencies required for judging authenticity of digital records by auditors were noted. Legislation that regulates records management, including digital records, was also reviewed to determine whether it is in a position to determine digital records' authenticity in order to support audit processes in the context of Botswana. Legislation was found to be available, although it has been found wanting. Lastly, the review assessed the role played by metadata in the maintenance of authentic records. This was in view of the fact that metadata is crucial in the management and preservation of records, as Franks and Kunde (2006:61) point out that it is the backbone of digital records management systems.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

The previous chapter reviewed literature related to the study. This chapter presents the research methodology adopted in this study. Ngulube (2015b:125) observes that the knowledge produced in the course of scientific research primarily depends on the research methodology. Research methodology refers to the way in which a research problem is resolved systematically (Kothari & Garg 2011:7). For Creswell (2014:34), research approach or methodology refers to the overall plan chosen to conduct research within which the researcher presents the intersection of the study research philosophy, research designs and specific methods employed. O'Sullivan, Rassel and Berner (2008:25) aver that research methodology has the following steps:

- Deciding when data would be collected and how.
- Development or selection of measures for each variable.
- Identification of study sample or test population.
- Making a choice of how study subjects would be chosen.
- Planning how data would be analysed.

The purpose of this study was to investigate the authentication of digital accounting records created through the GABS and to ascertain their authenticity for supporting audit processes in the public sector of Botswana. The methodology for the study is depicted in Figure 3.1.

3.2 Research Philosophy

Philosophical ideas in research remain largely hidden but they still influence the practice of research and therefore they need to be identified (Slife & Williams 1995). In agreement, Creswell (2014:33) advises that larger philosophical ideas need to be espoused, as such information justifies the choice of a particular research design or approach chosen. According to Rogers (2015:74), research involves philosophical assumptions about the nature of the world and the way in which we know the world, as well as choices of distinct methods or procedures. According to Creswell (2014:36), there are four identifiable research philosophies or paradigms. These are the following:

- **Positivist paradigm**: This is a scientific method. It is known as post-positivist research, empirical science and post-positivism. The term post-positivism challenges the traditional thought of positivism and its notion of absolute truth of knowledge. Post-positivism represents the thinking after positivism whereby there cannot be positivism about claims on knowledge while studying the behaviour and actions of humans (Creswell 2014:36).

- **Interpretivism**: The view of interpretivism is that individuals seek an understanding of the world around them by developing subjective meanings of their experiences towards certain objects or things socially and historically in life settings (Creswell 2014:37). Williamson (2013:7) describes it as an approach that is linked to naturalistic inquiry. Neuman (2014:4) indicates that by means of a systematic analysis of socially constructed meaning through an observation of people in their natural settings, one is able to arrive at an understanding of how people create and maintain their social worlds. This paradigm is seen as a typical approach to qualitative research (Williamson 2013:7; Thanh & Le Thanh 2015:25). The researcher unearths complex and varied views as understood through their situations and this is done through discussions with other persons. Subjective means are negotiated socially and historically through open-ended questionnaire enquiry.

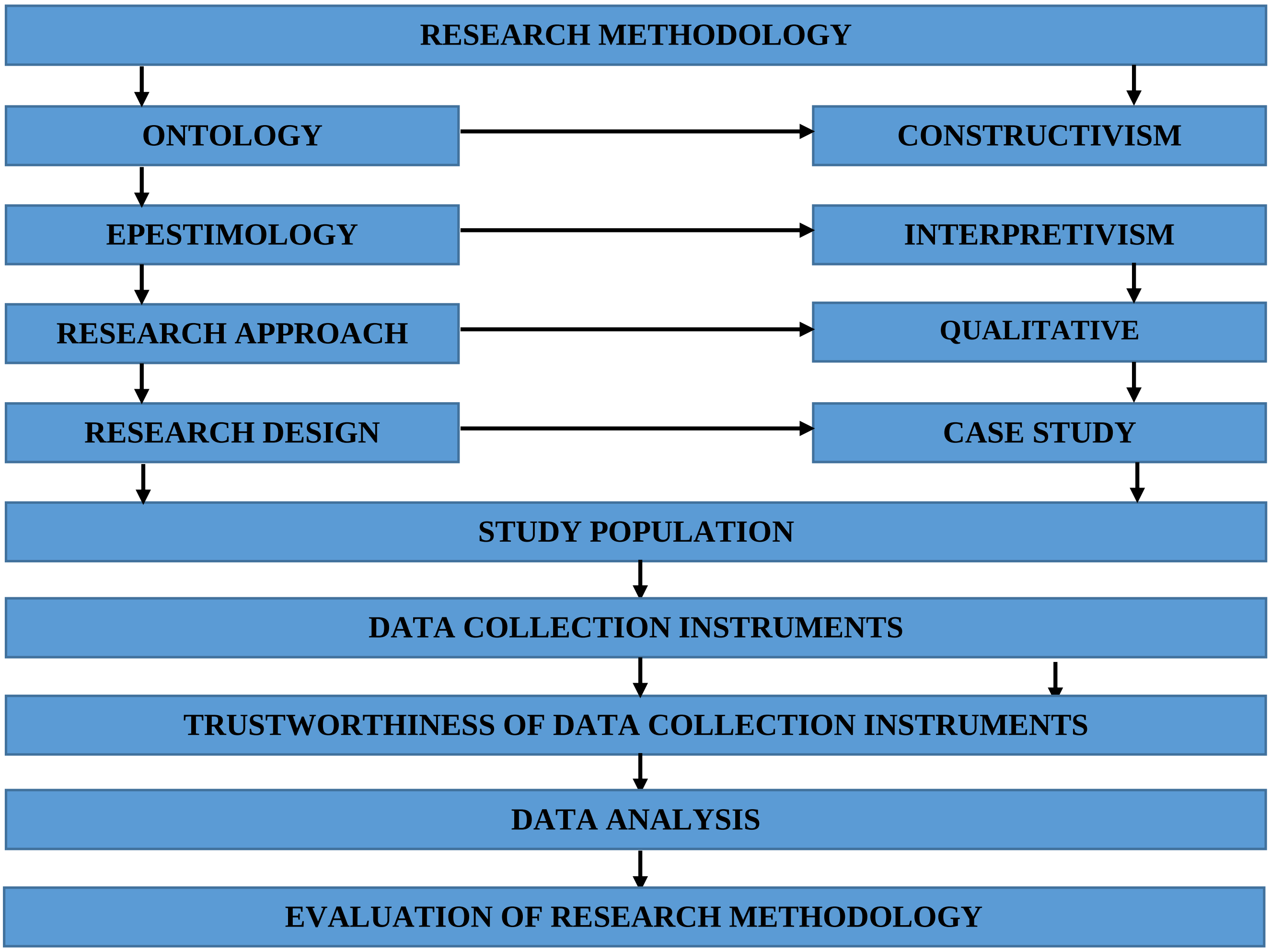


Figure 3.1: Research methodology for the study (Source: Field data 2018)

- **Transformative paradigm**: This view holds that research inquiry needs to be intertwined with politics and a political change agenda to confront social oppression at whatever levels it occurs, the result of which is an action agenda for reforms that may change the lives of the participants and the institutions in which individuals work or live, including the researchers themselves (Creswell 2014:38). This philosophical worldview mostly focuses on the needs of marginalised groups and individuals in society. Examples would be those who subscribe to feminist perspectives, racialised discourses, critical theory, queer theory and disability theory.

- **Pragmatist paradigm**: This research philosophy is better suited for answering the “what” and “how” research questions. Unlike post-positivism that concerns itself more with antecedents, pragmatism arises out of actions and situations (Creswell 2014:39). Its focus is the research problem and how it can be resolved, using various and applicable research approaches. According to Creswell (2009:10), pragmatism is usually associated with mixed methods research. It is a worldview based on actions, situations and consequences. Being more problem centred than philosophically centred, it puts less emphasis on methods and more on how best to resolve the research problem (Creswell 2009:10). Hence, it is receptive to multiple methods, different worldviews and different assumptions, as well as different forms of data collection and analysis (Creswell 2009:11).

3.2.1 Interpretivism

This study adopted interpretivism as an epistemology. Epistemology is about how we know what we know (Crotty 1998:8) or it concerns itself with how things get to be known and what is regarded as acceptable knowledge in a discipline (Walliman 2006:15; Tennis 2008:103). Epistemologically, the choice between two ways of acquiring knowledge is empiricism (knowledge gained by sensory experience thus using inductive reasoning) and rationalism (knowledge gained by reasoning thus using deductive reasoning (Walliman 2006:15). Epistemology is shaped by ontology (Williams & May 1996:69; Richards 2003:2). Ontology, on the other hand, is about the theory of social entities and is concerned with what exists to be investigated (Walliman 2006:15; Gray 2009:19). Bryman (2004:16-18) identifies objectivism (facts that have an independent existence) and constructionism (meaning is constructed through social interaction and is thus subjective). As an epistemology, interpretivism is linked to constructivism as an ontology (Lincoln & Guba 1985:37; Gray 2009:23). Crotty (1998:10) says these two are mutually dependent and difficult to distinguish when discussing research issues. This study adopts the understanding that “to talk about the construction of meaning (epistemology) is to talk of the construction of a meaningful reality (ontology)” (Crotty 1998:10). For this study, its ontology is constructivism and its epistemology is interpretivism.

This is similar to the view of Phiri (2016:111) who investigated the management of university records and documents in the world of governance, audit and risk in South Africa and Malawi.

Authors such as Willis (2007:90), Photongsunan (2010:3), Goldkuhl (2012:1), Creswell (2014:38), Thanh and Le Thanh (2015:25) opine that interpretivism is often associated with qualitative research. Interpretivism relies largely on the participants' views of the situation being studied (Creswell 2003:12). Meaning is constructed from responses offered by study respondents. According to Denzin and Lincoln (2005:22), research within the interpretivist paradigm is "is guided by the researcher's set of beliefs and feelings about the world and how it should be understood and studied." Benoliel (1996:407) asserts that within this paradigm, knowledge is viewed as being relative to circumstances that may be historical, temporal, cultural and subjective, and thus exists in multiple forms as a representation of reality, as interpreted by individuals. In the view of Willis (2007:194), it seeks answers to the research through various understandings of an individual's worldview as "different people and different groups have different perceptions of the world".

Compared to post-positivism, which is objective in nature, interpretivism research is more subjective than objective (Thanh & Le Thanh 2015:25). This makes sense, as subjectivity is central to forming meaning and understanding in research that involves human behaviour (Willis 2007:110). Through an interpretivist lens, researchers are able "to understand in depth the relationship of human beings to their environment and the part those people play in creating the social fabric of which they are a part" (McQueen 2002:17).

Authors such as Ritchie and Lewis (2003:23), Bryman (2012:650), Creswell (2014:36), and Thanh and Le Thanh (2015:25) are of the view that constructionism includes interpretivism within its realm. Others like Goldkuhl (2012:4) and Levers (2013:3) view interpretivism and constructionism as separate entities distinct from each other. According to Goldkuhl (2012:4), interpretivism can be classified into some categories or forms that can be termed as conservative, constructionist, critical and deconstructionist. Philosophically, this study fits in well with interpretivism as it adopts a case study design. It is exploratory in terms of research purpose and utilises the qualitative research approach. It mainly collects data using qualitative data collection instruments. It is thus fitting to use it to explore the authentication of digital accounting records in GABS in order to determine their authenticity for supporting audit processes in the public sector of Botswana. A study by Bushey (2016:112), which investigated the archival trustworthiness of digital photographs in social media platforms, also used archival diplomatics as a theoretical framework, employed the interpretivist worldview and used qualitative data collection and analysis. Creswell's (2014) categorisation of research paradigms is presented at Table 3.1.

Table 3.1: Summary of research paradigms (Creswell 2014:36)

Post-positivism	**Interpretivism**
• Reductionism • Determination • Empirical observation and measurement • Theory verification	• Understanding • Multiple participant meanings • Social and historical construction • Theory generation
Transformative	**Pragmatism**
• Political • Power and justice oriented • Collaborative • Change oriented	• Consequences of actions • Problem centred • Pluralistic • Real-world practice oriented

3.3 Research Approach

Literature on research methodology identifies three research approaches (Ngulube 2005:130; Creswell 2014:32; Johnson 2014:7; Ngulube & Ngulube 2015:1). These are quantitative, qualitative and mixed method research approaches. Quantitative research is based on the measurement of quantity or amount; hence, it expresses processes as a set of numbers (Rajasekar, Philominathan & Chinnathambi 2013:9). Its characteristics include but are not limited to the production of data in the form of numbers. It is non-descriptive, applies statistics and its results are often presented in the form of tables and graphs. Leedy and Ormrod (2005:135) opine that in terms of data collection methods, the quantitative research approach employs questionnaires, structured interviews and observations, secondary analysis and official statistics, coded content analysis, quasi-experiments and classic experiments.

Mixed methods research involves combining qualitative and quantitative research and data in a research study. This is based on the assumption that a mix of the two results in a more complete understanding of a research problem than either approach when used alone (Creswell 2014:32). Some scholars regard it as the third methodological movement (Teddlie & Tashakkori 2003: ix; Denzin 2008:4; Venkatesh, Brown & Bala 2013:22) that advocates for the usage of quantitative and qualitative approaches within a single study (Teddlie & Tashakkori, 2012:776; Wisdom, Cavaleri, Onwuegbuzie and Green 2012:723; Ngulube & Ngulube 2015:2). This study is principally qualitative in nature and used a qualitative research approach.

3.3.1 Qualitative Research Approach

Qualitative research is an approach for exploring and understanding the meaning that individuals or groups ascribe to a social or human problem (Creswell 2014:32). It is often based on interpretivism (Jupp 2006:342; Thanh & Le Thanh 2015:25) and the following are its characteristics: it is mainly concerned with the subjective meanings through which people interpret the world and construct reality through language, images and cultural artefacts in particular contexts; social events are from the perspective of the actors themselves independent of the researcher’s preconceptions. Qualitative research is conducted in a natural setting and involves a process of building a complex and holistic picture of the phenomenon of interest (Leedy & Ormrod 2005; Jupp 2006; Creswell 2007:37). Table 3.2 presents a comparison of qualitative and quantitative research approaches.

Table 3.2: Comparison of qualitative and quantitative research approaches (Bwalya 2011:230)

	Quantitative research	**Qualitative research**
General framework	Seeks to confirm hypothesis about phenomenon	Seeks to explore phenomenon
	Instruments use more rigid style of eliciting and categorising responses to questions	Instruments are more flexible, iterative of eliciting and categorises responses to questions in a more presentable manner
	Uses highly structured methods such as questionnaires, surveys and structured observations	Uses semi-structured methods such as in-depth interviews, focus groups and participant observation
Analytical objectives	To quantify variations	To describe variation
	To predict causal relationships	To describe and explain relationships
	To describe characteristics of a population	To describe individual/case experiences and to describe group norms
Question format	Closed ended	Open ended
Data format	Numerical, i.e. obtained by assigning numerical values to responses	Textual, i.e. obtained from audiotapes, videotapes and field notes
Flexibility in study design	Study design is stable from beginning to end	Some aspects of the study are flexible, for example, the addition, exclusion or wording of particular interview questions
	Participant responses do not influence or determine how and which questions researchers ask next	Participant responses affect/ determine how and which questions researchers ask next

	Study design is subject to statistical assumptions and conditions	Study design is iterative, i.e. data collection and research questions are adjusted to what is learnt

This study adopted the qualitative research approach and triangulation of data collection methods. This allowed the interpretation and understanding of research results (Bhebhe, Masuku & Ngulube 2013:50; Manewe-Sisa 2013:38; Maseh 2015:90; Marutha 2016:118). Aina (2002:23) defines data triangulation as “a process in research where different methods/techniques of data collection or sources of data are combined in a single study.” Data triangulation is widely accepted in empirical research by scholars and researchers (Yeasmin & Rahman 2012:154).

3.4 Research Design

Research is a well-planned activity. Research design refers to a procedural plan adopted by the researcher to answer questions validly, objectively, accurately and economically (Kumar 2011:96). Bryman (2012:46) describes a research design as a “framework for the collection and analysis of data.” For Bhattacherjee (2012:35), it is “a comprehensive plan for data collection in an empirical research project.” The same author describes it as a blueprint for empirical research for answering specific research questions and testing hypotheses. Minimally, it must at least have the following three processes:

- The data collection process
- The instrument development process
- The sampling process

According to Walliman (2011:9), various types of research designs are available for researchers and the one chosen depends on the nature of the research problems. Available to each research design are a number of different research methods commonly used to collect and analyse the type of data generated by the investigations. These research designs include experimental studies, case studies, historical studies, surveys, ethnography, action research and focus group research (Creswell 2003:13-16; Walliman 2011:9-13; Bhattacherjee 2012:38-40; Bernard 2013:216). This study adopted a single case study research design.

3.4.1 Case Study Research Design

This study is exploratory and utilises a case study research design. The system under investigation, GABS, is the case. Stake (1994:134) states that a case is a choice of what is studied analytically or holistically, entirely by repeated measures or hermeneutically, organically or culturally, using diverse methods. Stake (1995:135) describes a case as an “integrated system” bound by time and place. Using this analogy, Paré (2004:240) notes that a case may be a technology or system (e.g. GABS in this study) because it is an information system deployed and used as a working combination of ergonomic, technical and performance (e.g. response time) characteristics. Benbasat, Goldstein and Mead (1987:370) observe that in a case study, a phenomenon (GABS in this context) is examined in its natural setting, employing various methods of data collection to gather information from one or a few entities (people, groups or organisations).

In terms of research purpose, scientific research design can fall within the categories of exploratory, descriptive and explanatory research (Babbie 2007:87; Hernon & Schwartz 2009a:1). A case study can be situated with all of them. Yin (2009:18) defines a case study as “an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly defined.” A case explores real-life situations of a contemporary single or multiple case over time. It is detailed and gathers in-depth information using multiple data collection instruments (Yin 2009:2; Creswell 2013:97). Literature indicates that research includes both single and multiple case studies (Zainal 2007:2; Yin 2009:47; Gustafsson 2012:3). Within the two primary categories, Yin (2009:46) identifies four types of case study research designs, being single case studies, multiple case studies, holistic case studies and embedded case studies.

This study adopted a single case study design using five government departments selected from 24 mainline government ministries, among which five were quasi-government departments. The system under investigation, GABS, is the case studied. Further information on how the entities were chosen to take part in the study is presented under the sampling strategy used. Mosweu (2012) and Moatlhodi (2015) utilised case study research design in their investigations of the court records management system in the delivery of justice at Gaborone Magisterial District, Botswana, and e-records readiness at the Ministry of Labour and Home Affairs, respectively.

Case study research is applicable where a researcher endeavours to develop a theory from the data collected (Eisenhardt 1989:532; Eisenhardt & Graebner 2007; Moglia, Alexander & Perez 2011:2894; Ponelis 2015:536). This is because case studies enable the collection of rich, real-world context in which the phenomena are studied and, although sometimes seen as "subjective", a theory well built from case study research is surprisingly "objective" because its close adherence to the data keeps researchers "honest" (Eisenhardt & Graebner 2007:25). Eisenhardt and Graebner (2007:25-26) add that theory building from case study research is informed by the rich empirical data collected and thus enables a broader exploration of research questions and theoretical elaboration. A more accurate, interesting and testable theory is likely to be constructed from such data. A case study research design was appropriate for this study, as one of its objectives is to propose a framework for authenticating digital records in government accounting system to support audit processes in the public sector of Botswana.

3.5 Study Population

A study population refers to "the universe of cases and observation to which an argument refers" (Gerring 2012:431). For Hanlong and Larget (2011:7), a study population means all the individuals or units of interest. They add that not all individuals in a study population will have the data desired by the researcher in order to resolve the research problem. This is why there is a need to select study respondents through sampling. Ngulube (2005:133) 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 comprised of 24 mainline ministries of the government, inclusive of six quasi-government departments. The system under study, GABS, has been implemented in all government ministries and departments, including the quasi-government departments. The study population is presented in **Appendix 13.**

3.5.1 Sampling Procedures

Bhattacherjee (2012:65) refers to sampling as "the statistical process of selecting a subset (called a "sample") of a population of interest for making observations and statistical inferences about that population." Sampling is a common practice in empirical research. According to Ponto (2015:169) and Latham (2007:2), using a sample instead of the whole population is normally preferred because using the whole population is impossible due to the number of people, places or things within the population. It is comparatively cheaper, quicker and more practical to collect data from a representative sample of the population.

Sampling in the social and behavioural sciences can be broadly categorised into probability sampling, nonprobability sampling and systematic sampling design (Barreiro & Albandoz 2001:4; Kothari 2004:59-60; Teddlie & Yu 2007:77; Kumar 2011:181-190). On one hand, in probability sampling, each element in the population has an equal and independent chance of being selected like all others (Kumar 2011:181). Examples include simple random sampling, stratified random sampling and cluster sampling. On the other hand, Kumar (2011:187) attests that nonprobability sampling does not follow the theory of probability in the selection of the study sample as it uses elements in the population that are unknown or difficult to identify as individuals. Examples of nonprobability sampling designs include quota sampling, accidental sampling, judgemental sampling (purposive), expert sampling and snowball sampling (Kumar 2011:188; Singleton & Straits 2010:155-157).

From the study population derived from Botswana Telecommunications Corporation's telephone directory (Botswana Telecommunications 2017), six departments were purposively selected to take part in the study based on their function in the public sector of Botswana. Purposive sampling is associated with qualitative studies (Gentles, Charles, Ploeg & McKibbon 2015:1775; Padilla-Díaz 2015:104). The selected organisations taking part in the study were as follows:

- 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 moneys, 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: is 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 following studies, which focused on various aspects of archives and records management such as managing university records, digital records readiness, digital records management and digital court records management systems, also used purposive sampling to address the research problem (Kamatula 2010; Motlhasedi 2012; Moatlhodi 2015; Ngidi 2015). According to Kombo and Tromp (2006:82), with purposive sampling, the researcher selects participants on the basis of their ability to provide rich cases for in-depth analysis related to the central issues under study. Table 3.3 presents the purposively selected study respondents from the study population.

Table 3.3: Summary of study population and sample population

Government department/Ministry	**Sampled respondent(s)**	**Data collection tool**	**No of selected participants**
Department of Corporate Services (MFED)	Senior Records Manager Records Manager	Semi-structured Interview Semi-structured Interview	2
Department of Accountant General (AGD)	Records Manager Chief Systems Analyst Principal Systems Analyst (x2)	Interview Semi-structured Questionnaire Semi-structured Questionnaire	4
Department of Information and Technology (DIT)	Chief Systems Analyst Principal Systems Analyst	Semi-structured Questionnaire Semi-structured Questionnaire	2
Office of the Auditor General (OAGB)	Chief auditor: Central Government Principal auditor: Information Systems (x2) Principal Audit Officer Records Manager	Interview Semi-structured Questionnaire Semi-structured Questionnaire Semi-structured Questionnaire	5
Botswana National Archives and Records Services (BNARS)	Deputy Director: BNARS Head: Records Management Services	Interview Interview	2
Department of Internal Audit (DIA)	Chief internal auditor Principal internal auditor (x2)	Semi-structured Questionnaire Semi-structured Questionnaire	3
GRAND TOTAL NUMBER OF SELECTED STUDY RESPONDENTS			**25**

Source: Field data 2018

3.6 Data Collection Instruments

This study collected data using interviews, documentary review and system analysis. The first two is common in qualitative research as the study is principally qualitative (Creswell 2014:234; Ngulube 2015:8). System analysis was also used to collect data. It is a method of data collection common in computer science and information systems (Tutorials Point 2015:1). According to Case and Given (2016), qualitative studies tend to employ a multi-methods approach by using two or three sources of data from a mix of individual interviews, focus groups, observations, questionnaires and document analysis. The selected data sources enabled the researcher to collect extensive data on the event on which the investigation was focused (Leedy & Ormrod 2013:141). Combining data collection instruments, also known as triangulation, increases the validity of research by incorporating several viewpoints and methods (Yeasmin & Rahman 2012:156). It also helps to balance out, if not overcome, some of the challenges inherent in research of whatever methodological persuasion. The specific data collection instruments employed in the study are discussed in the next section.

3.6.1 Interviews

Interviews are a qualitative research technique whereby the researcher interviews a small number of respondents to explore their perspective of a particular idea, programme or situation (Boyce & Neale 2006:3). Saunders, Lewis and Thornhill (2012:372) define it as “a purposeful conversation between two or more people requiring the interviewer to establish rapport, to ask concise and unambiguous questions to which the interviewee is willing to respond and to listen attentively”. Three categories of interviews are identifiable in research (Burns 2000:582; Johnson & Christensen 2008:203; Knox & Burkard 2009:3; Fox 2009:5). These are structured (or standardised) interviews, semi-structured interviews and in-depth interviews. Authors do not agree on the number, as some include non-directive interviews, face-to-face interviews, telephone interviews and focus groups (Mathers, Fox & Hunn 2002:2-4; Kajornboon 2005:4; Cohen, Manion & Morrison 2007:352; Fox 2009:5-6). The differences between these categories lie in the structures and purposes of the interviews (Ngulube (2003:222) and a function of the sources read (Cohen et al. 2007:352).

Structured or standardised interviews are rigid, consist of closed-ended questions and are often used to ascertain facts presented to respondents in the same order (Fox & Burkard 2009:4). The interview questions are asked as prearranged throughout the interview with the use of standard probing. Alshengeeti (2014:40) observes that a structured interview is mostly organised around a set of predetermined direct questions that require immediate responses, mostly *yes* or no type. It is comparable to a self-administered quantitative questionnaire. Fox and Burkard (2009:4) argue that structured interviews have the advantage of uniformity in participant responses, but they limit the researcher in uncovering the participant's rich and unique experiences, especially those that lie outside the bounds of the interview questions themselves.

Unstructured interviews are highly flexible as they are open-ended (Alshengeeti 2014:40). There is a lot of freedom for both the researcher and interviewee in terms of planning, implementing and organising the interview content and questions (Gubrium & Holstein 2002:35). This allows the interviewer to follow up interesting developments while the interviewee is able to elaborate on various issues raised (Dörnyei 2007: 136).

Semi-structured interviews comprise "both elements of both quantifiable, fixed choice responding and facility to explore, and probe in more depth, certain areas of interest" (Brewerton & Millward 2001:70). According to Fox (2009:6), semi-structured interviews are similar to structured interviews in that for both of them, interview questions are pre-planned. The difference between these types of interviews is that for semi-structured interviews, the questions are open-ended and for structured interviews, the questions are closed ended. Semi-structured interviews are useful when studying a phenomenon which little is known about. This type of interview is a flexible form of the structured interview. It "allows depth to be achieved by providing the opportunity on the part of the interviewer to probe and expand the interviewee's responses" (Rubin & Rubin 2005:88). A checklist of interview questions was prepared prior to conducting the interview sessions. It allows for an "in-depth probing while permitting the interviewer to keep the interview within the parameters traced out by the aim of the study" (Berg 2007:39).

Although interviews offer some advantages in research, they also have some disadvantages. These include the following:

- They are time consuming and therefore take more time to complete.
- Interviews are also costly, as the researcher has to pay for the costs of travel to and from places where the interviewees are located.
- Interviewer bias is a danger that needs to be addressed.
- The researcher may not be able to discern the physical or emotional state of a participant (Adhabi & Anozie 2017:92)

For this study, the researcher utilised semi-structured interviews as they allow the researcher to further probe issues from the interviewee from the prearranged open-ended questions (Fox & Burkard 2009:3; Leedy & Ormrod 2013:190). The weaknesses of the interview method were addressed through the triangulation of data collection instruments whose advantages compensated for the weakness inherent in interviews.

3.6.2 Documentary Reviews

Documentary sources in the form of texts and documents provide useful data about society, both historically and the present (Walliman 2011:138). Document review in research means a way of collecting data through an evaluation of existing documents, both printed and digital (i.e. computer-based and internet-transmitted documents) (Bowen 2009:27; Department of Health and Human Sciences 2009:1). It is a study of created and available documents for purposes of deriving an understanding of the content or details and/or information covered (Ritchie & Lewis 2003:35). Wagner, Kawulich and Garner (2012:148) define it as an integrated and conceptually informed method of data collection that involves procedures and techniques for locating, identifying, retrieving and analysing documents for their relevance, significance and meaning.

Researchers often marginalise documentary research although it is as good as other commonly used research methods such as social surveys, in-depth interviews or participant observation (Ahmed 2010:2). It is commonly used to complement other data collection techniques (Ellison 2010:277; Ahmed 2010:2; Klein & Olbrech 2011:345). In a case study, Yin (2009:103) observes that document analysis plays a noteworthy role. Examples of documents that may be reviewed include archival documents, reports, programme logs, newspapers, newsletters, books, minutes, marketing materials (Department of Health and Human Sciences 2009:1; Ahmed 2010:2; Klein & Olbrech 2011:345).

As a data collection tool, documentary analysis has both advantages and disadvantages. The advantages are as follows:

- Information contained in extant document(s) is independently verifiable.
- The document review process can be done independently, without the need to solicit extensive input from other sources.
- Document review is typically less expensive.
- Eliminates researcher effect.
- Allows a larger sample.
- Contains spontaneous data.
- Enables access to information that would be difficult to get in any other way, for instance in an interview.
- Documents are often particularly useful for tracking change over time.
- Many documents can be of good quality and detailed.
- It provides a good source of background information.
- It provides a behind-the-scenes look at a programme that may not be directly observable (Bowen 2009:31; Department of Health and Human Sciences 2009:2; WBI Evaluation Group 2007:3; University of Portsmouth 2012)

The disadvantages are as follows:

- It depends a great deal on the researcher.
- It may be viewed as too subjective.
- Obtaining and analysing necessary documents can be a time-consuming process.
- Controlling the quality of data collected is beyond the researcher's control.
- Information may be inapplicable, disorganised, unavailable or out of date.
- Information could be biased because of selective survival of information.
  (WBI Evaluation Group 2007:3; Bowen 2009:32; Department of Health and Human Sciences 2009:2; University of Portsmouth 2012).

Just like the other data collection instruments, documentary analysis has some strengths and weaknesses. In this study, these were offset by triangulation documentary analysis with other data collection instruments. According to Katuu (2015), methods triangulation is useful in checking the consistency of research findings. Triangulation of evidence from different research methods is the ability to enhance the trustworthiness of an analysis by a fuller, more rounded account, reducing bias, compensating for the weakness of one method through the strength of another (Gorard & Taylor 2004:43). Denscombe (2007:138) further states that the use of triangulation validates research findings and alternative methods are used to confirm the accuracy of findings.

While the use of documentary analysis is widely accepted as a form of data collection in research, it is important to systematically handle the data in a similar way to when using other sources of data (Ahmed 2010:3). Cautionary measures should also be taken to verify the precision, accuracy and completeness of information presented (Bowen 2009:33). Researchers should not simply lift words and passages from available documents to be thrown into their research report without establishing the meaning communicated by the document as well as its general contribution to issues under exploration. According to Ahmed (2010:3), some kind of quality control criteria should be utilised prior to the use of documentary sources. Such criteria look at four factors being:

- Authenticity: This refers to whether the document is genuine.
- Credibility: This refers to the objective and subjective components of the believability of a source or message, whether the evidence is free from error and distortion.
- Representativeness: This refers to whether the document is typical of its kind or not, to the extent of its un-typicality known.
- Meaning: This refers to whether the evidence presented in the document is clear and unambiguous, such as whether the meaning conveyed is either a literal or face value meaning and an interpretative meaning (Denscombe 2007; Ahmed 2010:3-5).

This study reviewed a variety of documentary sources, which included newspapers, books, reports, policy documents, journal papers and legislative instruments, just to name a few. Studies by Ngoepe and Makhubela (2015), and Wamukoya and Mutula (2005b) used documentary analysis when investigating records management and the travesty of justice in South Africa, and capacity building requirements for digital records management practices in the ESARBICA region, respectively. The ESARBICA region is made up of countries in East and Southern Africa.

3.6.3 System Analysis

System analysis is the process of data collection and interpretation of facts, identifying problems and a decomposition of a system into its components. It is undertaken for purposes of studying a system or its constituent parts in order to identify its objectives (Tutorials Point 2015:1). According to Livari, Parsons and Wand (2006:510), the purpose of system analysis is to identify and document the requirements for an information system to support organisational activities. System analysis is part of the system development life cycle (SDLC) and provides answers to the questions "**Who** will use the system?", "W**hat** will the system do?" and "W**here** and **when** will it be used?" (Dennis, Wixom & Roth 2012:13). In the absence of a statement of user requirements (SOUR) for GABS, the researcher resorted to interviewing ICT specialists, some of whom performed the roles of system analyst to obtain information of capabilities of GABS for creating and storing authentic digital records. Users (accountants) were also interviewed to obtain the perspective of users. Documentary review is an accepted way of data collection in system analysis (Valacich & George 2017:150). Documentation such as copies of documentation relevant to GABS and its business processes was consulted. These pieces were documentation used to train users of GABS and were consulted by the researcher. An audit report on GABS by the Auditor General proved useful (Office of the Auditor General of Botswana 2007:20). The researcher could not use advanced methods of system analysis such as Joint Application Design (JAD), CASE tools, business process reengineering and prototyping (Valacich & George 2017:162-167) due to technical limitations.

3.7 Trustworthiness of Data Collection Instruments

While quantitative studies emphasise reliability and validity of research to ensure its authenticity and credibility (Golafshani 2003:597; Creswell 2014:201), qualitative studies employ trustworthiness of data collection instruments (Lincoln & Guba 1985:289-331; Shenton 2004:63; Baillie 2015:36). The criteria accepted for establishing the trustworthiness of qualitative research are as follows:

- **Credibility**: This means seeking to ensure that a study measures or tests what it is intended to measure or test (Kennedy-Clark 2012:5). This is the equivalent of validity in a quantitative-oriented study (Morrow 2005: 251; Baillie 2015:37). For this study, credibility was ensured through performing the following:
    a. ***Review of literature***: To evaluate whether study findings generally confirm past studies, as undertaking a good review of the existing body of knowledge is accepted as a crucial aspect for evaluating works of qualitative inquiry (Shenton 2004:69).
    b. ***Member checks***: This refers to cross-checking the accuracy of data collected either on the spot or at the end of the data collection process (Shenton 2004:68). For this study, the researcher asked the participants to repeat their assertions where clarity was needed on the side of the researcher to ensure that assertions are captured correctly.

c. ***Applying tactics to help ensure honesty in informants when contributing data***: For this study, as part of research ethics, participants were informed that taking part in the study was voluntary and participation was guided by free will on their part (Shenton 2004:66). In addition, they were encouraged to give honest answers to questions posed. Since they voluntarily agreed to take part, the researcher was confident that they provided accurate data. Ethical clearance was sought from the University of South Africa (Unisa) prior to the commencement of data collection.

d. ***The adoption of research methods well established both in qualitative investigation in general and in information science in particular***: According to Shenton (2004:64), this is achieved by employing specific procedures in data collection and analysis similar to those that have been done successfully in previous comparable studies. In this study, the researcher used methods and procedures in a way similar to earlier studies mentioned in the concluding paragraph in section 3.6.2.

e. ***Triangulation***: Using multiple sources of data is another way of ensuring credibility in a qualitative study (Shenton 2004:64). Accordingly, in this study, data collection instruments, such as documentary review and interviews were triangulated in order to complement each one with others and possibly cover up the weaknesses inherent in them.

- **Dependability**: This entails the notion that if the research is conducted in a similar context using similar data collection methods, then the findings should be similar (Kennedy-Clark 2012:5). It corresponds to reliability in a quantitative study (Morrow 2005:251; Baillie 2015:37). For this study, its dependability was promoted through formulating a research design which communicated to the reader the extent to which proper research practices were followed, including data collection instruments and the evaluation of data collection instruments in line with Shenton (2004:71-72). The researcher's promoter as attested to by Morrow (2005:252) and Amankwaa (2016:126) also examined the research report.

- **Transferability**: This means the extent to which the findings of the study can be applied to another study (Kennedy-Clark 2012:5). This is the equivalent of generalisability in quantitative studies (Morrow 2005: 251; Baillie 2015:37). In an attempt to enable this study to stand the test of transferability in qualitative studies, it observed Shenton's (2004:71) way of ensuring transferability. These include, from the onset, communicating (a) the number of organisations taking part in the study and where they are based; (b) any restrictions in the type of people who contributed data; (c) the number of participants involved in the fieldwork; (d) the data collection methods that were employed; (e) the number and length of the data collection sessions; (f) the time period over which the data were collected. In this study, this was done by providing this information in section 3.5.1, which presented sampling procedures. In addition, the data collection methods were presented before the study commenced. Lastly, being a case study, the findings cannot be generalised to the public service of Botswana as a whole. Amankwaa (2016:125) also states that transferability can be exercised through asking open-ended questions and conducting interviews that solicit detailed, thick and robust responses. This was done in this study.

- **Confirmabilit**y: This is where the researcher ensures that the findings of the study are the result of the ideas and experiences of the study participants, rather than the constructed ideas of the researcher (Gasson 2004:93; Morrow 2005:251; Kennedy-Clark 2012:5). In a quantitative study, it is referred to as objectivity (Connelly 2016:435). The assertion that "findings should represent, as far as is (humanly) possible, the situation being researched rather than the beliefs, pet theories, or biases of the researcher" (Gasson 2004:93). In this study, the research findings presented emanated from the assertions of the study participants. In addition, data triangulation was utilised to confirm findings and reduce them to the lowest possible issues of investigator bias. In addition, the study methodology and design were detailed under the research methodology chapter of the study in accordance with Shenton's (2004:72) line of thought.

According to Ngulube (2003:215), the quality of data collected in a study depends on the questions asked. It is therefore imperative that data collection instruments be pretested to deal with unavoidable human errors (Babbie & Mouton 2001:244; Bernard 2000:254). Although scholars agree that pretesting data collection instruments is a necessity in research, they do not agree on the number that can be sampled for the pre-test (Ngulube 2003:216). For example, Bradburn, Sudman and Wansink (2004: 317) suggest pretesting with at least with 10 to 12 colleagues or with representatives from the study population. Babbie (2007:257) feels that pretesting can be done with at least 10 participants. For this study, the data collection tools were pretested among 10 participants in the population who were requested to give their comments and inputs to fine-tune the collection tools, as also supported by Ngulube (2005:136). Data collection instruments were not pretested with participants within the study population because the researcher was of the view that those within the study population were likely to help improve them, as they were familiar with the study environment. The researcher supervisor also assessed the applicability of the data collection instruments to the study. The research supervisor is a seasoned researcher who has developed expertise in carrying out research.

It is of paramount importance in research to ensure that the research endeavour has trustworthiness, as it adds to the comprehensiveness and quality of the research product (Baillie 2015:36; Amankwaa 2016:8; Connelly 2016:436). This was with reference to the already mentioned aspects of ensuring the trustworthiness of data collection instruments in qualitative studies being transferability, conformability, dependability and credibility. Connelly (2016:436), however, contends that additional considerations for promoting trustworthiness such as ethical implications, research procedures that fit the research design and the way in which data are analysed should also be considered as they add on the quality of the research effort.

3.8 Data Analysis and Presentation

Qualitative interviews were the main method used in the study to obtain various perspectives on the research questions related to developing a framework for the authentication of digital records in a government accounting system to support audit processes in the public sector of Botswana. The analysis of qualitative data aims to describe some phenomena in detail (Flick 2013:5). The description can be about people, actions and events in their lives (Neuman 2011:507). The data collected helps the researcher to devise strategies for generating more data to answer the research question. Therefore, the focus of qualitative data is on the meaning of events and actions, not statistical significance, and the relationships between variables (Ngulube 2015:3). This study collected data in the form of document analysis, system analysis, email interviews and notes taken during semi-structured interviews. After the data were collected, it was systematically organised in accordance with research objectives, integrated and examined while searching for patterns or emerging themes (Alhojailan 2013:40), such that the research objectives which were turned into research questions became the major coding categories eventually broken down into subcategories (Ngulube 2015:5).

Data collected were analysed thematically (Braun & Clarke 2012:2). Thematic analysis involves identifying, analysing and reporting patterns (themes) emerging from data (Braun & Clarke 2006:79; Alhojailan 2013:40). It is generally the most widely used method of data analysis in qualitative research (Jugder 2016:2). According to Braun and Clarke (2006: 16-23), the process of thematic data analysis generally goes through the following steps:

- Familiarisation with data collected
- Generating initial codes
- Searching for themes
- Reviewing themes
- Defining and naming themes
- Producing a report

For this study, interviews were conducted face to face with some participants, but since they did not want to be recorded on tape, field notes were taken by hand. Then, after working through the collected data, more probing questions were asked during second interview meetings. The questions verified and confirmed interview responses from participants. In addition, for those participants who were not able to find time for face-to-face interviews, the interview questions were emailed to them and they responded to the questions. The researcher continuously asked follow-up questions for clarity. Participants were also requested to confirm some responses after they had been documented.

The data were grouped into themes that emanated from the research objectives. The same with data collected through system and documentary analysis. Data from the document analysis, interviews and system analysis were integrated in order to obtain a more holistic picture in an effort to provide answers posed by research questions.

3.9 Ethical Considerations

It is a requirement to follow proper and well-defined research in empirical research (Bwalya 2011:233). This study was conducted in a manner that observes expected ethical considerations as is the norm when conducting empirical research involving human participants (Powell & Connaway 2004:68; European Commission 2010:7; Unisa 2016:11; American Anthropological Association 2009:2-3). In line with the Unisa Policy on Research Ethics (UNISA 2016), the researcher observed the following:

- Obtained ethics clearance from Unisa’s Department of Information Science in the School of Arts, College of Human Sciences.
- Received clearance to conduct the study from the MFED, BNARS, the DIT and the Office of the Auditor General.
- Used the Unisa Policy on Research Ethics to guide the interaction between the researcher and research participants.

The following general ethics principles were taken into consideration during the conduct of this study (Unisa 2016);

- Existing literature related to the study was consulted to ensure that the study adds to existing knowledge.
- The study was conducted in a transparent manner, fairly and honestly by way of acknowledging information sources consulted.
- The research was undertaken as its results had the potential to benefit the Botswana public sector and as such, the results will be deposited with the Botswana National Library Services, the Botswana National Archives and Records Services as well as the Ministry of Finance and Economic Development libraries as a way to share the findings. Other than that, the study findings will be reported through publication in a journal(s) once the study is completed.
- Respect for and protection of the rights of study participants such as their right to preserve their dignity, privacy and confidentiality, including their institutions.
- Participation of study respondents was based on informed and non-coerced consent.

The applicable research ethics considerations were communicated to study participants. The issue of maintaining the privacy and confidentiality was addressed in this study by informing potential respondents that in order to conceal their identities, their names were not required in the data collection instruments, as also mentioned by Denzin and Lincoln (2000:139) and Creswell (2003:185). The researcher took care of the ethical principle of informed consent of participants by explaining the nature of the study in the data collection instrument and informed them that participation was voluntary. They were also urged to read them and sign the research participation consent form in line with the advice offered by Powell and Connaway (2004:187). However, the participants were encouraged to take part, as the study had the potential to be beneficial for the public sector of Botswana should the recommendations be implemented. It is an ethical obligation on the researcher to avoid fabrications and to not be fraudulent, as both of these are non-scientific and unethical (Denzin & Lincoln 2000:140). In this study, the researcher pretested the data collection instruments in order to ensure that they were accurate and could collect valid data required for interpreting the findings (Hurst, Arulogun, Owolabi, Akinyemi, Uvere, Warth & Ovbiagele 2015:3). Pretesting allows verification prior to actual data collection. It improves reliability and validity of findings and thus makes a research study rigorous (Morse, Barrett, Mayan, Olson & Spiers 2002:9).

3.10 Evaluation of Research Methodology

Research methods undertaken in a study can never be perfect, as attested by Leedy and Ormrod (2010: 285) and Ngulube (2005: 48). Such imperfections may place some doubt on the findings (Ngoepe 2012:115). This makes it necessary for the investigator to evaluate procedures involved in conducting the study in order to illuminate its weaknesses (Ngoepe 2012:116; Maluleka 2017:91).

This study utilised the qualitative approach and mainly triangulated data collection methods of document analysis, system analysis and interviews, with interviews as the dominant data collection tool. The triangulation of data collection instruments assisted in collecting reliable data and helped to offset the weaknesses of the individual data collection tools cited.

The investigator encountered challenges in data collection. The MFED, the mother ministry of the AGD, issued a research permit without a problem and formally informed the AGD about the research permit issuance in writing. However, authorities at the division managing GABS, the system under study, took much too long to allow data collection, as they did not initially understand the purpose of the study. The investigator had to explain the purpose of the study in detail and even resubmitted documents that were submitted for the application for a research permit at the MFED. Eventually, the researcher was allowed to interview selected participants.

The researcher had planned to tape record interviews, but that did not materialise as participants felt uncomfortable being recorded on tape. The researcher had to write down notes on the prepared semi-structure interview questionnaires. This disrupted the flow of the discussion, but the researcher worked around that by documenting responses and sending them back through email for the participant to crosscheck whether their assertions were captured correctly. Secondly, this allowed the researcher to pose more follow-up questions where there were gaps in the data collected. Participants duly provided the answers and emailed them back to the researcher.

Another challenge related to the purposive sampling of study participants. Initially, 18 participants were sampled to take part. Upon going into the field to collect data, it emerged that some questions would not be answered, as the right people to answer them were not sampled. The researcher was referred to those potential participants, as in snowball sampling. They included the Heads of Records Centres stationed at BNARS, an extra Records Manager at the MFED and Accountants who managed financial records at the MFED. This is why at the research design stage, a total of 18 participants were earmarked to take part in the study, but in the end, 25 took part.

The last challenge related to the timing of the data collection, which was the beginning of November 2017. This was a busy period as it was close to the end of the year with participants being too busy to schedule interviews. The researcher briefly met with those who could not find time for face-to-face interviews and explained the purpose of the study to them. They all agreed that the researcher should email them the semi-structured interview questions. The participants answered the questions and sent responses by email. Mostly, the researcher asked further follow-up questions through email, which ensured a lot of forward and backward communication between the researcher and the participants during the process of data collection. For some, probing questions were asked through telephone calls and answers given. Telephone calls were also used to contact participants to confirm some assertions.

3.11 Summary

This chapter outlined and justified the research design used to investigate how the authenticity of digital records in GABS is ensured to support audit processes in the public sector of Botswana. It also explained the rationale for utilising the selected data collection instruments (interviews and documentary reviews). The basis for the selection of the said data collection instruments was the research problem under investigation. The study population as well as the justification for adopting purposive and snowball sampling strategies have also been presented. This chapter also discussed measures employed to ensure the reliability and validity of data collection instruments, including ethical considerations for the study. The next chapter focuses on the presentation of results obtained from the selected data collection instruments.

CHAPTER FOUR

PRESENTATION OF DATA FINDINGS

4.1 Introduction

The previous chapter presented the research methodology applied in the pursuance of this study. Specifically, it covered methodological issues such as research paradigm and approach, research design, study population and sampling procedures, data collection and their trustworthiness, as well as ethical considerations for the study. This chapter presents the findings of the study as informed by research objectives in the endeavour to answer the research problem. Data presentation and analysis are crucial, as it enables the investigator to reduce data to an intelligible and interpretable form so that the relations of the research problem can be studied and tested, and conclusions drawn (De Vos, Fouche & Delport 2011:249).

The main purpose of this study was to develop a framework for the authentication of digital accounting records in a government accounting system to support audit processes in the public sector of Botswana. Accordingly, this chapter presents the study findings from data gathered from the field by the researcher in a logical and sufficient manner (Blum 2006:2), in order to enable the researcher to answer the research questions (Creswell 2009:152).

4.2 Background of Participants

Qualitative studies do not place much emphasis on response rates and sample representativeness, as the results of the study cannot be generalised to the public sector of Botswana as a whole. According to Neuman (2006:219), in qualitative studies, researchers focus more on how the sample, cases, units or activities illuminate social life and less on representativeness. Participants for the study were selected using both purposive and snowball sampling strategies. The response rate is not reported, as this is a qualitative study. In his study, Maluleka (2017:95) also did not report on the response rate as the study was qualitative and its findings could not be generalised, just like the current study. Table 4.1 presents participant work designations and their place of work.

Table 4.1: Participant work designations and their place of work

Department	Participant job designation	Number
Botswana National Archives and Records Services	Head: Archives Administration Head: Records Management Services Principal Records Managers II x 3	5
Department of Internal Audit	Principal internal auditor Senior internal auditor Internal auditor x2	4
Department of Information Technology	Chief Systems Analyst Chief Programmer Systems Analyst	3
Office of Auditor General	Auditors x5 Senior auditor	6
Accountant General's Department	Chief Accountant Senior Accountant Accountant Principal Finance Officer Principal Accounts Officer	7
Ministry of Finance and Economic Development HQ	Principal Records Manager Records Manager I	2
TOTAL		**25**

Source: Field data (2018)

The profile of study participants in terms of their designation in their work roles indicates that there is a mix of senior and junior officers. This suggests that with experience, one becomes knowledgeable in their work and the responses to the study questions are reflected in their years of experience. This served the study well.

4.2.1 Educational Background of Participants and their Work Experience

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 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.

4.3 Data presentation

This study collected qualitative data from the semi-structured interviews, documentary reviews and system analysis. Qualitative data were collected, and emerging themes were analysed thematically and presented in a narrative form. According to Braun and Clarke (2006:4-5), thematic analysis should be seen as a foundational method for qualitative data analysis. Due to its theoretical freedom, it provides a flexible and useful research tool with the potential to provide a rich and detailed account of complex data. The presentation of the data was guided by the study objectives, which were to:

- analyse the legislative framework for the creation of authentic, reliable digital records stored in GABS in support of audit processes in the public sector of Botswana
- find procedures in place to maintain the authenticity of digital accounting records created and stored in GABS
- establish skills and competencies needed by auditors, ICT specialists and records managers to establish the authenticity and reliability of digital records created and stored in GABS

- determine how digital records created and stored through GABS are managed as authentic and reliable to support audit processes in the public sector of Botswana
- propose a framework for ensuring that authentic reliable records are created and stored in GABS to support audit processes in the public sector of Botswana.

4.3.1 The Legislative Framework for Authentic and Reliable Digital Records

The first objective of the study sought to analyse the legislative framework for the creation of authentic, reliable digital records stored in GABS in support of audit processes in the public sector of Botswana**.** An analysis of the Laws of Botswana Online revealed the following as the main legislative and policy framework that regulates the management of records in the public sector of Botswana. Study participants also identified the same legislation, policies and procedures. Table 4.2 presents the legislative framework analysed.

Table 4.2: Legislative framework

Legislation	Year
Constitution of Botswana, Cap 0000, Sections 117 and 124.	1966
National Archives and Records Services Act, Cap 59:04	1978 (Amended in 2007)
Electronic Records (Evidence) Act	2014
Electronic Records (Evidence) Regulations	2016
Electronic Communications and Transactions Act	2014
Electronic Communications and Transactions Act Regulations	2016
Public Audit Act, Cap 54:02	2012
Public Finance Management Act	2011
Cybercrime and Computer Related Crimes Act, Cap 08:06	2007
Criminal Procedure and Evidence Act, Cap 08:02	2004
National ICT Policy	2007
National e-Government Strategy	2011

Source: Field data 2018

The legislative and policy framework presented in Table 4.2 is discussed in detail in the sections that follow. The discussion borders on the status of the legislation and policies in terms of providing guidance for the management of digital records with a particular focus on the authentication of digital records in GABS to support the audit process in the public sector of Botswana.

4.3.1.1 Constitution of Botswana

The Constitution of Botswana (Government of Botswana 1966) is the supreme law of the country. All laws should promote its spirit and become unconstitutional if they contract its provisions. Section 117 indicates that "all revenues or other moneys raised or received for the purposes of the Government of Botswana (not being revenues or other moneys that are payable by or under any law into some other fund established for a specific purpose or that may by or under any law be retained by the department of the government that received them for the purposes of defraying the expenses of that department) shall be paid into and form one Consolidated Fund." The auditing of government financial statements is therefore a constitutional requirement, the mandate of which is performed by the Office of the Auditor General of Botswana.

Section 124(1), (2), (3) and (5) established the Office of the Auditor General of Botswana. It annually audits public accounts and reports the findings to Parliament through the Minister of Finance and Economic Development. The Constitution prescribes that the Auditor General should be given access to all books, records, reports and other documents relating to those accounts for auditing. When exercising such constitutional functions, the Auditor General should not be directed or controlled by anyone or authority. In essence, the Constitution promotes accountability and transparency in the use of state financial resources. This can be obtained through the Office of the Auditor General having uninhibited access to financial records emanating from the expenditure of government departments during audits. Secondly, such records (i.e. books, records, reports and other documents) have to be complete lest they are useless in the audit process.

4.3.1.2 National Archives and Records Services Act

The study found that the principal legislation regulating records, regardless of form or format, in the public sector of Botswana is the National Archives and Records Services Act. It was initially enacted in 1978. In 2007, its definition was expanded to include digital records. This legislation only goes as far as that extension and does not provide more guidance on how the management and maintenance of authentic digital records should be carried out. The amendment also legally gave BNARS the mandate to oversee the management of public sector records across their whole life cycle, including digital records produced in various e-government systems across government ministries and departments. Previously, the mandate of BNARS was archives administration. Suffice to say that digital accounting records created and stored with GABS fall within the ambit of BNARS in terms of their management over time.

Specifically, the mandate of BNARS to manage public sector records, inclusive of digital accounting records transacted through GABS and stored in it has been explicitly stated as follows:

- Section 5 (2), which designates the Director of BNARS as the principal administrative officer in charge of the department and the custodian of public archives. In this context, public archives refer to public records that possess historical or enduring value, have been transferred to the national archives or place of deposit, including those acquired for purposes of this the National Archives and Records Services Act. Public archives also mean records in the custody of a government department.
- Section 5(4) mandates the Director of BNARS to accept, store, preserve, describe and arrange all public archives transferred to it. It also mandates BNARS to advise government departments and ministries on the proper care, preservation, custody and control of public records. In addition, this Act provides for the making and authentication of copies of and extracts from public archives required as evidence in legal proceedings or for any other purpose approved by the Minister.

In practice, the efficiency and effectiveness of the government machinery are promoted generally if:

- records management is considered a business process designed to support business objectives
- records are considered a resource and are utilised fully to realise business objectives
- each governmental body creates and maintains a culture which promotes proper records management to facilitate efficient and timely decision-making (Ngoepe 2012:75).

Records management professionals were interviewed on issues related to the role played by BNARS in ensuring that digital records management and the availability of standards and guidelines in place to promote the creation and maintenance of authentic digital records and the coverage of records authenticity in legislation and policies. Data from interviews with records management personnel at BNARS indicated that they are aware of the current legislative framework governing records management. When it comes to the role played by BNARS in ensuring that digital records produced by various information systems are created authentically and maintained as such for as long as they are needed, their responses suggest that the department is not practically doing so well in that regard. Their responses on the role played by BNARS in the management of authentic public sector records are presented at Table 4.3. Throughout this chapter, the following codes have been used to represent the study participants.

Key: AG1-5: Auditors at Office of Auditor General of Botswana
IA1- 4: Internal auditors at Department of Internal Audit
ICT1-5: ICT specialists
RM1-5: Records Management Professionals

Table 4.3: BNARS' role in ensuring the creation and maintenance of authentic digital records

Participant	Response
RM1	*Through the e-government records management cluster, BNARS is currently trying to find a footing on realising this feat*
RM2	*Yes. The Botswana National Archives and Records Services under the Ministry of Youth Empowerment, Sport and Culture Development is the managing/coordinating partner for the Electronic Records Management and Library E-Government initiatives. Records management considerations for electronic records management have been submitted to the e-Government Cluster to be used for guiding the kind of system which would be suitable for proper electronic records management*
RM3	*Currently, BNARS is working on the National Archives and Records Management System (NARMS) project to create an environment that governs records created electronically, this includes authenticity of digital records.*
RM4	*There are legal frameworks which govern the entire public sector in creation of records like the BNARS Act of 1978 which was revised in 07. Part VI talks of Validity, Evidence and Copyright this is where issues of access and destruction. There are also Regulations which goes with this Act where there are penalties. There is also Electronic Records (Evidence) Act which also governs the electronic records*
RM5	*BNARS maintains that all public sector records should be managed in compliance with the BNARS Act and Regulations as well as other related Acts (Electronic Evidence Act). The Act does not state the format of records, therefore this means that, currently, all records that are system generated should be printed and manually filed accordingly*

Source: Field data 2018

The assertions by records management professionals in terms of the role played by BNARS in ensuring that digital records remain authentic after creation are typical in that they generally point to the current incapacity of BNARS to provide guidance for the managing of digital records. Notably, there are ongoing efforts to address this challenge through the implementation of NARMS, a system meant to properly manage digital records created in government ministries and departments until such records become archives. Thereafter, such records are to be transferred to BNARS to be ingested into archival custody.

4.3.1.2.2 Standards and guidelines for authentic digital records

Participants were also asked about the availability of standards and guidelines in place to promote the creation and maintenance of authentic digital records in the public sector. The question was posed to records managers at both BNARS and the MFED (mother ministry of the AGD, which is the custodian of GABS). The responses are presented at Table 4.4.

Table 4.4: Standards and guidelines for promoting digital records authenticity

Participant	Response
RM1	*Guidelines on conventional records only*
RM2	*National Archives and Records Services Regulations of 2012* *Generic Classification Scheme of 2009* *Generic Records Retention & Disposition Scheme of 2009* *Generic Records Management Policy of 2009*
RM3	*The International Records Management Standards, ISO 15489:1-2*
RM4	*The Electronic Records (Evidence) Act recognises electronic signatures and these helps to ensure authenticity of digital records*
RM5	*Currently, an electronic records management strategy is being developed to guide Government on Management of Electronic Records. Currently, we have an email management draft guideline to assist in email management*
RM6	*There are no standards and guidelines in place in guidance of creation and maintenance of authentic digital records.*
RM7	*There are no guidelines that guide digital records instead there are general guidelines that govern records as whole*

It is notable that the guiding documents cited by the records management professionals provide guidance for paper records at the exclusion of digital records. This was highlighted by **RM6** who said that, "there are no standards and guidelines in place in guidance of creation and maintenance of authentic digital records." As for ISO 15489-1 (2016), records management professionals at BNARS indicated that, although it was yet to be domesticated, it was used as is to guide public sector records management. Its adoption has not been formalised therefore it is used as guiding tool and reference point.

4.3.1.2.3 Provision of records authenticity in legislation and policies

The records management personnel were also asked the extent to which the authenticity of digital records is addressed by available legislation that related to digital records management. The participants' responses are presented at Table 4.5.

Table 4.5: Coverage of records authenticity in legislation and policies

Participant	Response
RM1	*Not adequately addressed, the existing framework is only skewed towards process, methods, and systems and enforced by BOCRA*
RM2	*The issue of digital records authenticity is not adequately addressed by the available legislation.* *There is no electronic records management policy in the country* *There are efforts to ensure authenticating electronic records through the Electronic Records (Evidence) Act which deals specifically with computer generated data or records produced by electronic systems and the authentication of such evidence*
RM3	*I am not aware of any legislation to that regard*
RM4	*The existing legislations do not go in too much detail like sometimes there are no regulations which provide more details*
RM5	*The area of digital/electronic records is still unchartered, there is an Electronic Evidence Act and it has no regulations, therefore, there is still*

	more to do on addressing issues of authenticity. However, the Act does advocate that electronic/digital records can be used as evidence in the court of Law.
RM6	*The legislation and policies do not address for recognition of digital records and authenticity of electronic documents*
RM7	*I am not sure if digital records authenticity is covered adequately in law*

Source: Field data 2018

The findings reveal that although some laws cover the authenticity of digital records such as the Electronic Records (Evidence) Act and the Electronic Telecommunications Act, generally, the records managers lack that awareness. One mentioned, "there is an Electronic Records (Evidence) Act and it has no regulations", although the truth of the matter is that the law has some regulations which actually operationalised it. Ngoepe and Saurombe (2016:29-30) acknowledge that the expansion of the word "record" in the National Archives and Records Services Act to include a digital record helps to ensure that as many forms of records as possible are included. However, Ngoepe and Saurombe (2016) as well as Ngoepe and Keakopa (2011:155) still argue that the legislation is still inadequate to deal with managing records in a cloud environment. For example, Ngoepe and Saurombe (2016:29-30) contend that, although the Minister responsible for the archives and records management portfolio is legally mandated to declare any place a place of deposit, questions such as whether the Minister has the capacity to determine such a place suitable, the legal obligations of the declaration and the legal capacity of the Minister and Director to monitor the cloud for violations should they occur still remain unanswered.

4.3.1.3 Public Audit Act

The Public Audit Act empowers the Auditor General of Botswana to go through any records, books or other documents in any public office or give instruction for that to happen. He has access to all offices, stores or premises that fall under his audit powers. He may charge for auditing the accounts of any public offices. After two months of the end of every financial year, each person who was responsible for any accounts during that year should prepare, sign and transmit a report of such account to the Auditor General and the Accountant General in a form directed by the Minister of Finance. Section 11(2) of the Act mandates the Accountant General to transmit to the Auditor General accounts and statements of that financial year six months after the end of the financial year and (also those specified in the Public Finance Management Act for him to audit them) as the Minister of finance may specify. When the Auditor General has examined the accounts and statements, he returns them, together with a certificate, to the Accountant General who will submit them to the minister of finance within four weeks. Within 30 days of receiving the accounts, statements and the certificate, the Minister of Finance will present them to the National Assembly. It is the duty of the Auditor General to gather the necessary tools to implement or establish auditing standards, and his activities have to be based on those standards and also have to make sure that any people under the auditing function comply with those standards. He is also responsible for establishing a quality control system to make sure that the auditing standards are followed in the audit field and ensure that the standards are suitable and applied consistently.

The Auditor General produces a report, which includes opinions and statements relevant to the person/entity audited, on every audit that he carries out. The report also has to touch on:

- the financial position at a specific date, results of operations and cash flow for the period which ended on that date conforming to the applicable financial reporting framework and legislation
- compliance with any legislation by the audited person in relation to finances
- reported information relating to the performance of the audited person against predetermined objectives.

The Auditor General must forward his reports after auditing the accounts and statements to the Minister of Finance within nine months after the end of the relevant financial year or within three months after receiving the accounts and statements form the Accountant General. The Minister of Finance shall present the reports (unaltered) from the Auditor General to the

National Assembly within 30 days of receiving them. If, for whatever reason, the minister fails to deliver the reports to the National Assembly, the Auditor General can send them to the Speaker and the Speaker will present them to the National Assembly. The Auditor General has the power to audit any account and he or any person authorised to audit such has to disclose any findings, including unauthorised expenditure or any misconducts relating to the audited account. However, the Auditor General will not disclose any information that is protected by any Act of Parliament and also he cannot release any information that he obtained in the course of his work, unless the information is required by the DCEC in relation to any investigation or by a court which has a competent authority to interpret and apply the law.

Section 13(1-6) gives the Auditor General the authority to audit the books of accounts of public interest organisations if deemed to be in the best interest of the public to do so. Public interest organisations are those organisations jointly owned by the government and another party with government owning 51%. In carrying out the investigations, the Auditor General "shall be entitled to make copies of, or take extracts from any such records" (page 95). In the process of auditing the books of accounts, it is a requirement that complete and truthful records be made accessible in accordance with section 4 of the Act.

Section 18 of PPA indicates that auditing in the public service of Botswana should conform to auditing standards, both internationally and locally. From interviews with auditors, it emerged that the public service of Botswana conforms to auditing standards as issued by the International Federation of Accountants and the International Auditing and Assurance Board (International Federation of Accountants 2015).

Once an audit is completed, an audit opinion has to be tendered and that is a requirement of section 19, which specifically prescribes that an audit report has to be issued to an auditee and it should reflect at least an opinion or conclusion on:

- whether the annual financial statements of the auditee fairly present, in all material respects, the financial position at a specific date and the results of its operations and cash flow for the period which ended on that date in accordance with the applicable financial framework and legislation

- the auditee’s compliance with any applicable legislation relating to financial matters, financial management and other related matters
- the reported information relating to the performance of the auditee against predetermined objectives.

In addition, the Auditor General may report on whether the auditee’s resources were procured economically and utilised efficiently and effectively.

4.3.1.4 The Electronic Records (Evidence) Act

The Electronic Records (Evidence) Act (Government of Botswana 2014a) was enacted as part of reforms towards developing cyber legislation in Botswana (Keetshabe 2015). Principally, it was enacted to legalise the admissibility of digital records as evidence in legal proceedings and authentication of digital records. Primarily, the Act does not invalidate any law that has been passed in relation to the allowance of digital records in legal proceedings besides the rules relating to validity and quality of that evidence. The rules of evidence do not restrict the production of a digital record as evidence only, because it is a digital record. The court has the liberty to look at evidence produced under this Act when applying common law rules that relate to the allowance of digital records. A person is allowed to produce a copy or an extract from a book or record in digital form in any legal proceedings, irrespective of the provisions of section 244 of the Criminal Procedure and Evidence Act, which requires signed and certified copies, extracts and records. Any person who produces a digital record as evidence has to prove that the evidence is genuine by producing evidence that will support that the digital record he or she produced is what he or she implied it to be. A government official who possesses some records by nature of his or her office shall produce them as digital records before the court in civil or criminal proceedings as ordered by the Directorate of Public Prosecutions (DPP).

An extract from a banker’s book is sufficient to be produced in digital form and it will be regarded as the original record. Whoever wishes to produce a digital record as evidence of entry in a banker’s book has to do it in accordance with the proviso to section 248 (1) of the Criminal Procedure and Evidence Act. Section 6(1) of the Act defines an approved process as a process approved by a Certifying Authority, being the Communications Regulatory Authority in this Act, according to the provisions of any regulations made by the minister. Where a digital record is produced as evidence, the record must be allowed if it is relevant and produced in an approved manner, unless it is stated otherwise in any other written Act. The certifying authority will sign and issue a certificate to identify the digital record system and also the part of it that is relevant to the proceedings, which will be enough evidence of the ethical code of the digital record system. A record shall be presumed to accurately reproduce the contents of the original record if the record has been obtained from a digital record system certified by the certifying authority unless proven otherwise.

A person holding a responsible position is the one who can sign the certificates issued in the matters mentioned in accordance with subsection 3, which shall be found as enough evidence of the matters given in the certificate. Any digital record brought forth as valid evidence will be allowed as proof of the contents of the original records besides the fact that it is secondary evidence and that some features of the original are missing in the record as long as they do not affect the accuracy of the relevant records. The best digital evidence rule will depend on the proof of the integrity of the digital record system in which the digital record was stored. Furthermore, if there was a digital signature, it could be used to verify whether the digital record has not been changed ever since it was made. A printout digital record will satisfy the best evidence rule if it has been previously used as a record of the information recorded or stored in the printout. In cases where a signature is required, or certain consequences attached if the record is not signed, a digital signature will satisfy such requirement.

Where the law requires one’s signature but is not specific as to the type of signature, the use of a digital signature shall meet that requirement. Where evidence of the integrity of a digital records system is missing, any evidence can be used that can support that the computer system or any device that was used by the digital records system was operating properly or, if it was not operating properly, it did not affect the integrity of the digital records system and there is no reason to doubt its integrity. The person offering that record can also prove that there is no reason to doubt the accuracy of the digital record due to the improper use of the digital records system. The integrity of a digital records system can also be proven by establishing that the record was stored by someone who is opposing the interests of someone who wants to introduce it and establishing that the record was stored in the normal business manner by a person who was not under any pressure from the person who wanted to introduce it. To determine under any rule of law as to the admissibility of digital record, the evidence can be provided pertaining to any standard, procedure, usage or practice in which the records are recorded or stored, bearing in mind the type of business, enterprise or endeavour that used, recorded or stored the digital record and, lastly, the nature and purpose of the digital record. An affidavit may be provided for the aforementioned matters as yet another proof to support the given evidence.

Where the court is not satisfied with the accuracy of evidence provided under section 4 of this Act, it may request further evidence. Where further evidence has been requested, that evidence can be supported by an affidavit that is made by a person holding a responsible position in the management or operation of the Certifying Authority or any other person who is responsible for the operation of the digital records system at that time or the person who had control over or access to any relevant records or facts in relation to the production of the digital record or a person who had obtained or been given access to or control over any relevant records or facts in relation to the production of the digital record or an expert appointed or accepted by the court. The court may require that oral evidence be given concerning the validity of digital records and may call a deponent of an affidavit under section 12(2) or any person responsible for a certificate issued under section 6 of this Act, to give oral evidence. The court can assess the weight of any digital record produced under section 5 by looking at the circumstances from which any conclusion can be made regarding the validity of the digital record and also whether or not the information was supplied to or derived from the relevant digital system or recorded with the aim of being supplied to it, not leaving out the facts contained in the information and also whether any person involved in the supplying and processing of such information had any motive to give inaccurate information.

4.3.1.5 The Electronic Communications and Transactions Act

The Electronic Communications and Transactions Act (ECT Act) was enacted in 2014 to provide for the facilitation and the regulation of digital communications and transactions, specifically to regulate digital commerce and digital signatures. The law recognises digital communication; therefore, information would not be denied validity, legal effect and enforcement just because it is digital information or because it is not contained in the digital communication which intends to give rise to a legal effect, but it is only referred to in that digital communication. In terms of this Act, a digital signature will not be denied legal effect or declared invalid just because it is in digital form. If the law requires a person's signature and all the requirements are met with regard to any digital communication or transactions performed, including a demonstrated ability to identify the owner of the signature, then the signature is duly accepted for authenticating information used in the digital transaction. This rule will apply even if the law attaches consequences if the signature is not provided as required.

Where the original form of information is required, a digital communication would be enough if there is proof of the integrity of the information from when it was generated until it reached its final form as digital communication or else it would have to be assessed, and also if the information can be easily displayed to the person whom it has to be presented to. In assessing the integrity of the information, it would be ensured that no alterations were made to the information besides any additions made in the normal course of communication, its storage and display and also the main reason why the information was generated. The assessment would apply even if the law created any consequences in cases of non-compliance. Conforming to the Electronic Records (Evidence) Act, evidence rules would not hinder digital communication from being produced as evidence only because it is a digital communication or because it is not the original form of that evidence, more especially if it was the only best evidence that the person could produce.

Information that is brought in digital form is assessed and given weight in relation to how reliable the way is in which the data was generated, stored and communicated. This includes the reliability of the way in which the integrity of the digital communication was maintained as well as the manner in which the originator of the data was identified. Lastly, any other relevant circumstances are considered. A person can use digital communication if he or she is required to hand in certain documents or information only if the information in the digital communication can be easily accessed for reference or if the communication is presented in the same format in which it was generated, sent or received or if the format gives the accurate information and, lastly, if the origin, destination, date and time of the sending and receiving of the digital communication can be determined. All the above-mentioned apply when a person was obliged to hand in the information or when there are consequences attached to failure to hand in the information.

Where the law requires a person to produce a document or information, digital communication is sufficient if, at the time the digital communication was sent, there was reasonable belief that the information in that communication would be readily available when accessed for reference purposes or if the integrity of the information could be easily proved. The integrity of the document will be assessed by checking whether the information has been kept complete or it has been altered, besides any additions or changes that occurred in the normal course of communication, storage and even display. A contract can be made through digital communication and the contract will not be denied enforceability only because it was made through digital communication, either in whole or in part; however, a proposal concluding a contract that is addressed to different parties using different digital communications, not to a specific person, will be considered an invitation to make offers, unless it is clearly indicated in the intention of the person making the proposal to be bound in case of acceptance.

With regard to the use of automated message systems, a contract between a person and an automated message system or between two automated message systems is considered legally enforceable or valid even if no natural person interfered with them. A digital signature is considered reliable and sufficient if its creation data are only linked to the person who has signed and nobody else, or if, at the time it was signed, the signature creation data was only controlled by the person who has signed, or if it can be detected that some alteration was made to the signature after the time of signing, or if the requirement of the signature is a way to prove the integrity of the information. in which case it has to be detectable if the signature has been altered after the time of signing. However, those requirements do not limit the ability of a person to bring forward any proof of the unreliability of a signature or to establish its reliability. The Minister may provide any services that will help recognise secure digital signatures. The Communications Regulatory Authority is responsible for recognising foreign certificates and every method prescribed here will be recognised internationally. Where a secure digital signature has been provided, it will be regarded as a valid digital signature unless the opposite is proved.

There are factors to be considered to determine the security and reliability of any systems used by service providers:

- Assets, financial and human resources
- The quality of the hardware and software systems
- Procedures used for processing certificates, applications for the certificates and preserving of the records
- Availability of information to people who have signed and been identified in certificates or potential relying partners
- How often the procedures and records are audited and an existence of a declaration with regard to compliance with any factor or even any other factor

In finding out if the digital signature or certificate is valid, the location where the certificate was issued or the digital signature was used is not important or even the business location of the issuer or the person who signed. It does not matter if the certificate was issued in or outside

Botswana, they are both valid if they give the same level of reliability and the same applies for a signature used in or outside Botswana. The certificates or digital signatures are said to have the same standard of reliability if they are recognised internationally.

The agreement of parties on what certificates or types of signatures they want to use is sufficient as long as they are not prohibited by the applicable legislation. Part VI of the Act only applies to digital transactions, but not through auction; supply of daily food items or beverages commonly used in households; fluctuating prices that cannot be controlled by the supplier; services which began with the consumer's consent before the end of 7 days; where goods are made according to consumer's specifications and desires or cannot be returned or they easily rot and are likely to expire every now and then; where media files or computer software was opened by the consumer; sale of books, periodicals or newspapers; provision of gaming services; online gambling; and for the provision of leisure services where upon the conclusion of transaction the supplier has to deliver the services within a specified date.

4.3.1.6 Electronic Communications and transactions Act Regulations

Electronic Communications and Transactions Act of 2014 has regulations which came into effect in 2016. They operationalised the ECT Act. Sections 3, 4 and 5 regulate the application of digital signature service providers, licence issuance and renewal. The Botswana Communications Regulatory Authority (BOCRA) is the organisation responsible for issuing such licences. Section 9 of the Act sets out requirements to be met by certification service providers who wish to provide products or services required to authenticate and recognise secure digital signatures.

4.3.1.7 Public Finance Management Act

The PFMA, Act No. 17 of 2011, was enacted to make provision for the control and management of public moneys and supplies, and for matters connected therewith and incidental thereto. Together with the Constitution and the Public Audit Act, the PFMA provides the cornerstone of the broad legal framework for public finance management (European Commission Delegation Botswana 2009:28). Section 4 of the Act prescribes that the Minister responsible for finance has to ensure full accountability for public finances in terms of their supervision, control and direction. Section 9 of the Act provides for the classification of accounts and the basis for accounting to be done and to conform to professional accounting standards as set by an accounting recognised in Botswana, including compliance with national and international best practices with respect to public finance accounting.

Section 13 of the Act lays down the powers and duties of the Accountant General as a public officer and they include in the context of this study, the following:

- Compilation and management of the accounts of government
- Custody and safety of public moneys
- Disbursement of public moneys
- Issuing of procedures and guidelines for the control, custody, issue and use of public moneys

Section 53 of the Act recognises that the PFMA may have some regulations which may authorise the use of digital forms, signatures and approval processes and procedures. This includes digital transactions in general terms, keeping books of accounts and other digital records as and when transactions are conducted within GABS. Currently, there are no such regulations in place.

4.3.1.8 Cybercrime and Computer Related Crimes Act

This piece of legislation was enacted in 2007 for purposes of combating cybercrime and computer-related crimes and to deal with criminal activities perpetrated through computer systems as well as to collect digital evidence for the prosecution of such crimes (Government of Botswana 2007). The Act defines a computer or computer system as “an electronic, magnetic or optical device or a group of interconnected or related services, including the internet, one or more of which, pursuant to a programme, performs automatic processing of data or any other function." GABS fits in well in this definition and is thus a computer system as it performs automated transactions that deal with accounting decisions.

The Act also defines data as

a. "Any representation of facts, information or concepts in a form suitable for processing in a computer or computer system"
b. "Any information recorded in a form in which it can be processed by equipment operating automatically in response to instruction given for that purpose."
c. "A programme suitable to cause a computer or computer system to perform a function."

Section 4 of the Act shows that a person will be guilty of an offence when he or she accesses a computer system or part of it without the permission to do so or when he or she causes the computer system to perform any function due to the fact that he or she was not given the authority to access it. The punishment is a fine that is less than or equivalent to P10 000 or imprisonment of less than or equal to six months and, in some cases, the punishment can be both the fine and imprisonment. A person will not be found guilty if he or she had a right to control the computer or computer system and also did so in good faith; the person was given oral or written consent by a person with the power to authorise him or her to access the computer or computer system; he or she actually had a reason to believe that he was given consent to access the computer or computer system; the person acted in conformance to the measures mentioned in part III of the Act; or if the person was acting in accordance with a written Act or authority given to him or her by that Act to obtain information or possess a document or some property. Therefore, it is illegal for anyone to get unauthorised access to a computer system and fiddle with records in its database. In this case, it is unlawful for unauthorised persons to authorise access to GABS.

A person is said to be unauthorised to have access to a computer or computer system when he has no right to access the item in question or does not have consent from a person who actually has the right to access that item or the person actually exceeds the access that he or she was given permission to. Whether or not the person who had unauthorised access to a computer or computer system did not target a certain programme or data in the computer is irrelevant; the fact remains that they accessed that computer of computer system without valid permission. A person will be found guilty of an offence if they do not have the permission to access a computer or computer system or they exceed the permission they were given with the aim of obtaining a computer service directly or indirectly, or directly or indirectly causing any function or data of the computer or computer system to be diverted in some way. If a person is charged with the previously mentioned offence, they would go to prison for a term less than or equal to one year or the person would have to pay a fine of less than or equivalent to P20 000 and, in some cases, both. Where the data in the computer or computer system are altered or the operation is impaired, the punishment is increased to P40 000 and two years' imprisonment.

It is does not matter if the unauthorised access or diversion was not aimed at certain data or programme in the computer or computer system. A person would not be found guilty of the latter offense if he has written or even oral permission from the sender of the data and the person who was supposed to receive the data or if the person was acting with the power given to him or her by any written Act. Accessing any data or programme held in a computer or computer system or accessing a computer service with the intention of committing an unlawful act is a crime in its own and one can be imprisoned for less than or exactly six months or pay a fine less than or equivalent to P10 000. However, it does not matter that the access was permitted or not or even that the offence was further committed at the same time as when access was secured or just any other time. Any person who deletes, destroys or alters data or renders the data meaningless or ineffective, or interferes with the lawful usage of that data or even the person associated with the lawful usage of data, or denies anyone entitled to access that data the right to access it will be guilty of an offence and can face a minimum term of six months imprisonment, but the maximum not greater than two years, or may face the payment of a fine amounting to a minimum of P10 000 but not greater than P40 000 and, in some cases, the punishment can be both.

If the operation of the computer or computer system is impaired, suppressed or altered and the same occurs for the access to any programme or data in the computer or computer system, even the operation of any programme or the reliability of any data, all as a result of committing any of the latter offences, the culprit may pay a fine of not more than P20 000 or may serve less than one year in prison or both. However, a person would not be found guilty where the person’s action is conforming to the measures provided in Part III of this Act and also where the person acted under the authority given to him or her by any written law to get any document or property or access to information. Interference is not permitted if the person causing it is not entitled to determine if the interference should be made or where the person does not have permission from a person who has the authority to cause the interference. It does not matter if the unauthorised interference or any intended impact of it is permanent or temporary. A person who intentionally interferes with the functioning of a computer or computer system or with the person who is lawfully operating a computer or computer system will be guilty of an offence and will pay a fine that is not more than P5 000 or will serve a term not more than three months in prison or both. Interfering with a computer or computer system includes cutting electricity supply to, causing electromagnetic interference to or corrupting by any means the computer system and also inputting, deleting or altering data and impairing the connectivity of a computer system. A person who commits an act which directly or indirectly causes denial of access to or any impairment to the programme or data stored in the computer system, whether partial or complete, is guilty of an offense and can be sentenced to a minimum of six months or a maximum of two years in prison or pay a fine equivalent to P10 000 but not greater than P40 000, or both.

Any person who technically deflects a non-public transmission to, from or within a computer system or diverts electromagnetic emissions that are carrying data without any lawful excuse commits an offence and may be faced with a term of six months or more but not greater than two years or may pay a fine of P10 000 or more but not exceeding P40 000 if found guilty, or both. A person who avails a computer system or any device without any lawful excuse in order to commit a crime under this Act commits an offence and shall be liable to a fine less than or equivalent to P20 000 or an imprisonment term of less than or equivalent to one year, or both.

A person who receives or possesses any device as described previously without any lawful excuse commits an offence and shall be liable to a fine less than equivalent to P20 000 or an imprisonment term of less than or equivalent to one year, or both. If one is found having any data or programme without any unlawful excuse, intending to use such data or programme or for someone else to use such to commit any offence under this Act, the person will be guilty of an offence and shall be liable to a fine less than or equivalent to P20 000 or an imprisonment term of less than or equivalent to one year, or both. Possession of any data or programme would include that of a computer system or device containing such programme or data, having a document where the data are recorded, or having control of the data or programme that someone else has.

Any person who avails a password, access code or any way in which data can be reached in the computer system for unlawful purposes knowing that it might cause harm to any person will be committing an offence and shall be liable to a fine less than or equivalent to P10 000 or an imprisonment term of less than or equivalent to six months, or both. Any person who causes the introduction of a computer contaminant or introduces such contaminant which causes or is capable of causing damage to the computer commits an offence and will pay a fine not less than P40 000 but not greater than P100 000 or serve a minimum imprisonment term of two years but not more than three years if found guilty, or both. A contaminant includes any programme that alters, destroys, records or transmits any data that are contained in the computer; seizes the normal operation of the computer; or affects the performance of the computer in any way, for example, connecting it to another computer resource in such a way that when the computer operates, the same instruction is carried out in the other computer. Any person who produces false data so that it can be believed to be genuine (forging data) is committing an offence and shall be liable to a fine less than or equivalent to P20 000 or an imprisonment term of less than or equivalent to one year, or both. Any person who intentionally favours himself or herself or any other person by fraudulently causing another person to lose property by deleting or altering data or interfering with the functioning of a computer will be committing an offence and shall be liable to a fine less than or equivalent to P20 000 or an imprisonment term of less than or equivalent to one year, or both.

In short, one would say the CCRCA does protect digital records or data and their authenticity and states steps to take against anyone who tempers with them. Just as paper records, forging digital data is a crime. It discourages any acts of data manipulation with heavy fines.

4.3.1.9 Criminal Procedure and Evidence Act

The purpose of the Criminal Procedure and Evidence Act is to make provisions with respect to procedure and evidence in criminal cases and to provide for other matters related to such evidence and procedures (Government of Botswana 1939). It was last amended in 2005. Section 244 regulates documentary evidence tendered in court, specifically certified copies or extracts of documents admissible. It says that for any book or public document to be admissible as evidence before a magistrate or court on any preparatory examination, it should be retrieved from the custody of the officer entrusted with its custody. It should be proved that it was indeed an examined extract or copy. Alternatively, it can only be admissible if it can be proved that it has been certified as a true copy or extract by an officer who has been given custodial responsibilities over its original.

Section 246(2) indicates that a copy or extract certified to be such shall be admissible before any court or magistrate holding a preparatory examination and carry the same value and weight just like its original counterpart. Section 246(3) prescribes that as, an individual, the Head of Department or Office does not need to produce an original document all the time, but can authorise an officer under his control to produce. However, for a certified copy or extract, any party who wants it to be accepted by the court as evidence to argue their case can produce it.

4.3.2 Procedures for Authenticating Digital Accounting Records

The second objective of the study was to find procedures in place to maintain the authenticity of digital accounting records created and stored in GABS. Some of the subsections were posed to records management professionals, ICT professionals and auditors and these related to procedures for the creation and maintenance of digital records in information systems, GABS inclusive.

4.3.2.1 Records authenticity assessment in GABS

The theoretical perspective used to evaluate whether GABS created and maintained authentic digital accounting records was archival diplomatics, which provides a specified view of a model record. This includes the means of understanding and defining record authenticity, including elements that comprise it (McKemmish & Gilliland 2013:101). A record that is authentic has its identity established and its integrity demonstrated (MacNeil 2002:1). InterPARES (2002) benchmark requirements for establishing records authenticity enumerate basic characteristics of a trusted record-keeping system which has rules that control the creation, maintenance and use of the creator’s records, and that support a presumption of the records in the system.

Central to the assessment of records authenticity in digital systems are identity and integrity metadata (InterPARES 2002:5-7; Duranti & Blanchette 2004:2; Duranti 2014). Rogers (2015d: 14) says that the principles of archival diplomatics are used to identify records in digital systems, including an assessment of their authenticity. Other than that, Duranti and Blanchette (2004:2) aver that in archival theory, a component of archival diplomatics, records used to transact organisational business are regarded as authentic.

These findings reveal that the identity of records (a component of records authenticity) created through GABS can be established because the system is able to capture and store the following core information or metadata about digital records that are persistently linked to it over time and across hardware and software platforms for purposes of establishing and perpetuating its identity. The metadata alluded to include the following:

- Name of author
- Addressee

- Writer
- Manifestation of the record’s archival bond
- Indication of the action or matter to which the created record relates
- Indications of any attachments or annotations

Archival diplomatics theorises that for records to be deemed authentic, their identity has to be established. In this regard, records in GABS are identifiable, but this does not mean they are authentic, because their integrity also needs to be determined if they are to be regarded as authentic. Furthermore, since GABS was implemented in 2004, its software platforms have been updated to the latest version consistently. The current version is called Oracle E-Business Suite. The system has also been migrated to the latest hardware that supports its operations.

ICT professionals were also asked to give their views on the availability of procedures in GABS against the InterPARES benchmark requirements for assessing records authenticity. The participants’ responses were translated into ticks and all of them ticked all the procedures for records authenticity as present. The procedures are actually the system controls at database level and the application controls at the business function level. The results of the GABS assessment against the InterPARES (2002) Benchmark requirements for assessing records authenticity are presented in Table 4.6. The responses were obtained from ICT1, ICT2, ICT3 and ICT4 from the DIT who also serve GABS System Support ICT specialists. Table 4.6 presents the evaluation results of GABS against the InterPARES benchmark requirements for assessing records authenticity in information systems.

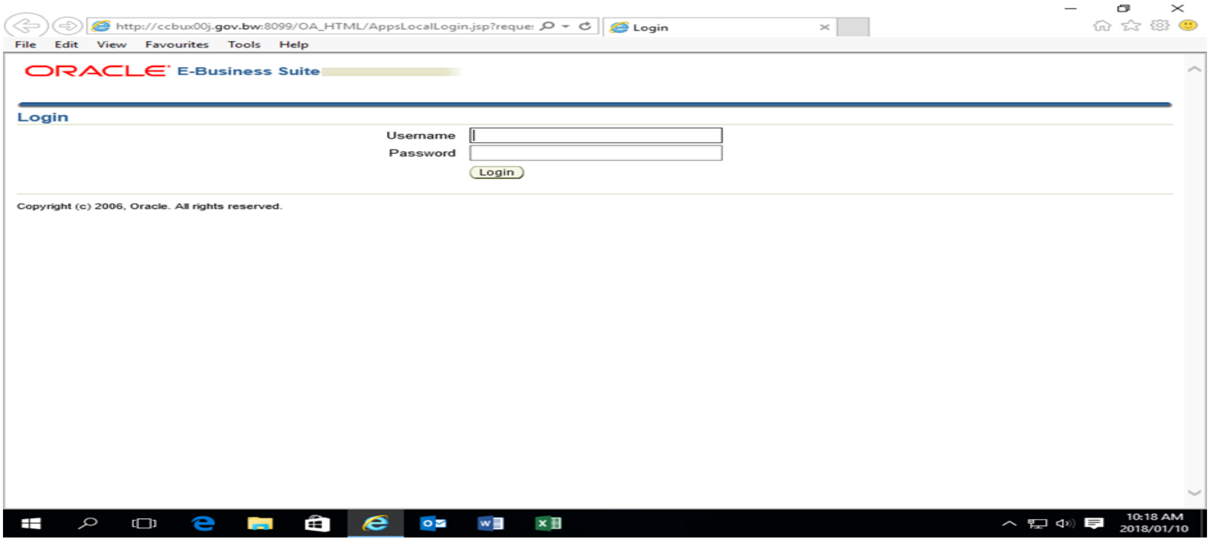
Table 4.6: Benchmark requirements for assessing records authenticity in GABS

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 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: Field data 2018

The findings are consistent with archival diplomatics in terms of records authenticity as theorised by InterPARES, because these findings indicate that the integrity of records in GABS has been established. This is consistent with MacNeil (2002:7) who says that controls in an information system can “provide a circumstantial probability of their integrity.” Furthermore, Figures 4.1 and 4.2 present the GABS interface for gaining access into the system and another one, which shows the segregation of duties within the system.



http://ccbux00j.gov.bw:8099/OA_HTML/AppsLocalLogin.jsp?reque
Login
File Edit View Favourites Tools Help
ORACLE E-Business Suite
10:18 AM
2018/01/10

Login

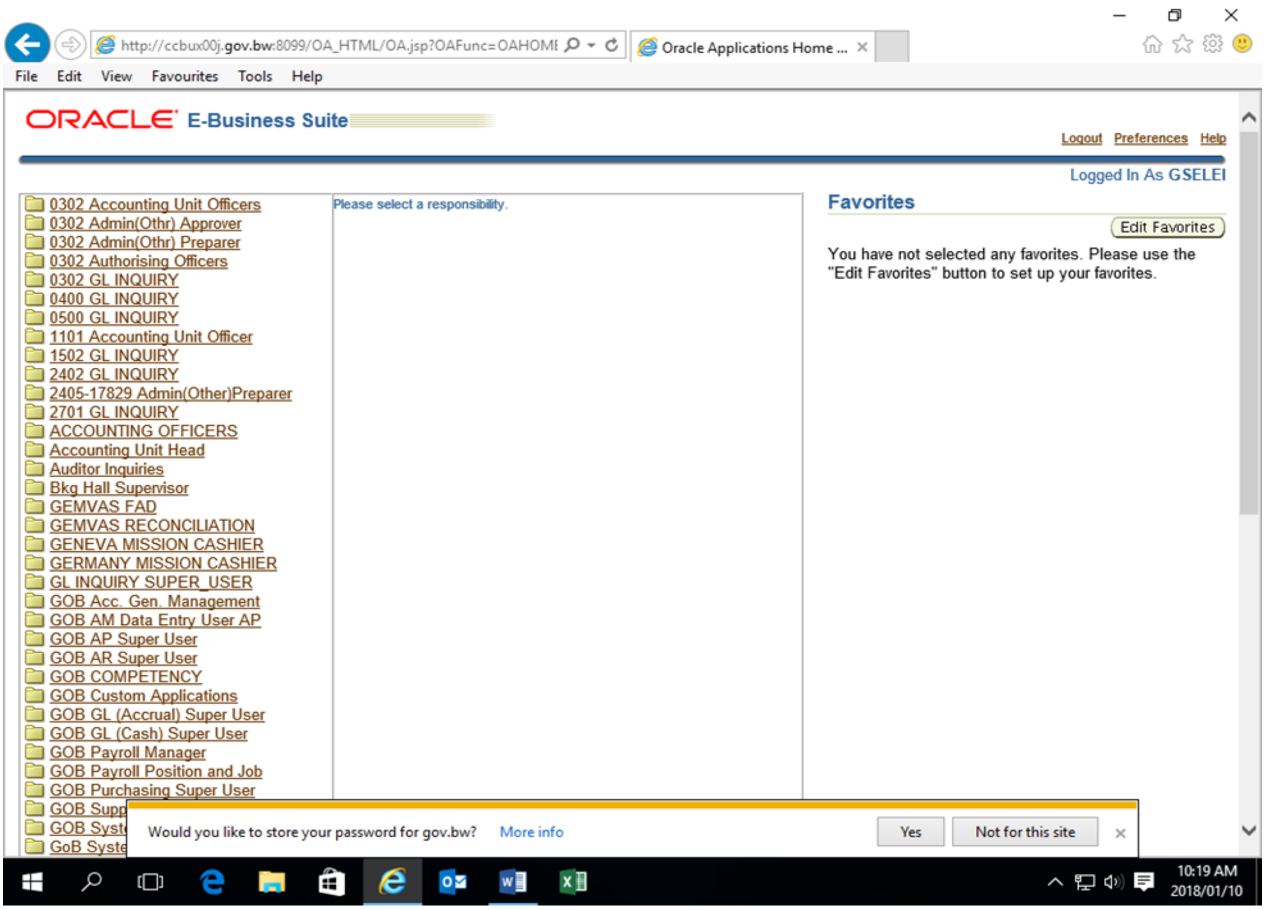
Username

Password

Login

Copyright (c) 2006, Oracle. All rights reserved.

Figure 4.1: Gabs Log in interface



http://ccbux00j.gov.bw:8099/OA_HTML/OA.jsp?OAFunc=OAHOME
Oracle Applications Home ...
File Edit View Favourites Tools Help
ORACLE E-Business Suite
Logout Preferences Help
10:19 AM
2018/01/10

Logged In As GSELEI

- 0302 Accounting Unit Officers
- 0302 Admin(Othr) Approver
- 0302 Admin(Othr) Preparer
- 0302 Authorising Officers
- 0302 GL INQUIRY
- 0400 GL INQUIRY
- 0500 GL INQUIRY
- 1101 Accounting Unit Officer
- 1502 GL INQUIRY
- 2402 GL INQUIRY
- 2405-17829 Admin(Other)Preparer
- 2701 GL INQUIRY
- ACCOUNTING OFFICERS
- Accounting Unit Head
- Auditor Inquiries
- Bkg Hall Supervisor
- GEMVAS FAD
- GEMVAS RECONCILIATION
- GENEVA MISSION CASHIER
- GERMANY MISSION CASHIER
- GL INQUIRY SUPER_USER
- GOB Acc. Gen. Management
- GOB AM Data Entry User AP
- GOB AP Super User
- GOB AR Super User
- GOB COMPETENCY
- GOB Custom Applications
- GOB GL (Accrual) Super User
- GOB GL (Cash) Super User
- GOB Payroll Manager
- GOB Payroll Position and Job
- GOB Purchasing Super User
- GOB Supp
- GOB Syst
- GoB Syste

Please select a responsibility.

Favorites

Edit Favorites

You have not selected any favorites. Please use the "Edit Favorites" button to set up your favorites.

Would you like to store your password for gov.bw? More info Yes Not for this site

Figure 4.2: Interface for the segregation of duties in GABS

The findings from the system analysis also revealed that, as theorised by archival diplomatics, records in GABS have the following identifiable characteristics:

- **Fixed documentary form**: Once a record is created in GABS, it cannot be deleted or modified. If such a record does not represent a transaction truthfully, it is made in a sort of image or shadow, then a correct record is created and both exist in the system. These procedures are controlled. An action officer who discovers a record that does not provide truthful evidence of the transaction it forms a part of, the officer can only report such discovery. Another officer can then deal with it by turning it into a shadow in the system. The system of roles and responsibilities tied to performing transactions in the system governs the whole situation. In essence, records in GABS are fixed and cannot be changed and this fits in well with the character of a record as looked at with an archival diplomatics lens.

- **Stable content**: This refers to the message communicated or conveyed by the record. Various financial transactions are carried through the system and the records serve as evidence of the very same transactions. Stable content means that the entity's content must remain fixed and complete with no chance of being altered when in storage and the message it conveys remains unchanged and just like when it was first produced to transact business (Duranti & Jansen 2011:3).

- **Archival bond**: This refers to the relationship that links each record to the previous one and the subsequent one (Duranti 2001:273). Transactions in GABS related to others within and outside the system. For example, at the start of every financial year, budgeting is done and recorded in manual records. Once the budget is approved, it is captured onto the system. Thereafter, expenditure is recorded in the system following a system of requests and approvals and these are done both in the system and outside of it (in the paper counterpart).

- **Juridical-administrative context**: GABS operates within the confines of legislation applicable to financial management and control. These include the Public Finance Management Act, Public Audit Act and the Constitution of the Republic of Botswana.

- **Procedural context**: It is made up of business procedure in the course of which a record is created. There are various procedures in GABS, and these relate to, among others, imprest application, payment to suppliers and application for per diem. For example, a procedure should be followed when an officer requests for per diem to go on a trip outside the country. It involves trip requisition, approval up to the payment of money into the travelling public officer's bank account.

- **Provenancial:** This refers to the creating body, its mandate, structure and functions. In this case, the creating body is the AGD, which is the principal government entity entrusted with financial management and control through GABS.

- **Technological context:** This is defined as the characteristics of the technological components of a digital computing system in which records are created (Catto 2006:7). GABS is based on a standard Enterprise Resource Planning (ERP) package, Oracle Financials. It was customised to meet the needs of the user department, being AGD. Modules normally not found in a standard ERP such as a Public Debt Unit function and the Revenue Office Data Capture Module were added during customisation.

4.3.2.2 Procedures for creating and maintaining authentic digital records

Records managers at BNARS were also asked whether the institution has 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. A similar question was asked of records managers based at the MFED. It enquired about whether the MFED has developed procedures for ensuring the creation and maintenance of authentic reliable digital accounting records created and stored in GABS. The responses are presented in Table 4.7.

Table 4.7: Procedures for creating and maintaining authentic digital records

Participant	Response
RM1	*It is within BNARS strategy to engage with other strategic partners and also in line with Government Modernization Office (e-government) to have policies, strategies that speak to new trends of archives and records management. Recently, the BNARS through MYSC took part in the Government of Botswana Enterprise Architecture a direction towards assessing all available systems with a view to streamline discrete systems. This will in the long run, I believe, enhance a focused approach to developing regulations and policies that are not fragmented.*
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 applicable in all government.*
RM3	*None that I am aware of.*
RM4	*Systems in government, their servers are maintained and stored by the Department of Information Technology. There are no procedures in place.*
RM5	*BNARS currently is more focused on management of physical records as they are the most created by Ministries and Departments. This means that as system-generated records are printed, then 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 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.*

Source: Field data 2018

The findings show that despite BNARS being mandated by the National Archives and Records Services Act to be the leading government agency in the management of records, including digital records, it is yet to develop and implement procedures for ensuring that digital records generated by various information systems in government remain authentic for as long as needed. BNARS has only issued procedures for the management of paper records.

4.3.2.3 Ability of GABS to create and maintain records authenticity

A few questions based on procedures for ensuring authentic digital records were posed to internal auditors coded as IA1, IA2, IA3 and IA4. The first sub-question was on the extent to which GABS as a system possessed the ability to capture, protect and maintain authentic digital accounting records that are reliable and accessible if needed. The responses are presented at Table 4.8.

Table 4.8: Ability of GABS to create and maintain records authenticity

Participant	Response
IA1	*From tables that we access from GABS for purposes of auditing, we noticed that data integrity is compromised as evidenced by incomplete records. Some fields which could be mandatory are sometimes left unpopulated.*
IA2	*Data is captured by front officers, then validated by supervisors before being saved on the database. Employees are assigned roles on the system and only allowed to perform those roles. The database has administrators who maintain applications running on the database to ensure that data is accessible anytime, and also secure data on the database to ensure that it is only accessible to authorised personnel. Data is stored at one place (data centre) which has a physical security to entry. There are also network firewalls to protect unauthorised access.*
IA3	*Audit was granted data access and interfaced our audit tool with GABS, so we download our data straight from GABS; therefore, we can conclude that the data is reliable. We have access to data downloading as and when needed, though naming of tables on GABS is very vague.*

IA4	*Partial, data can be edited or deleted and required fields populated with incorrect data.*

Source: Field data 2018

From the perspective of the internal auditors, the findings of the study show that GABS have good general computer controls and system application controls that can facilitate the protection of digital records in GABS once created and stored in the system. It is also clear that any negligence by both users and administrators can expose the records to possibilities of tampering, erasure or deletion. In such a case, the authenticity of records in the system would be at risk. Such records would not be acceptable to auditors in the audit process.

4.3.2.4 Criteria for declaring records authentic and reliable

The second sub-question was: "What criteria are used by auditors to conclude that digital records in an information (such as) GABS have maintained their identity and integrity (authenticity) and reliability?" Both auditors responded to it from the Department of Internal Audit and Office of the Auditor General of Botswana. The responses are presented in Table 4.9.

Table 4.9: Auditor criteria for authenticating digital records

Participant	Response
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 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 data analytical tool (ACL) 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 test such as IsBlank. The tests can be tests of data formats and blank fields of required or mandatory fields.*
AG1	*Data extraction should be done in the presence of auditors. Integrity checks are performed first through 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.*
AG2	*By tracing the transactions in the financial statement backwards to the initial stage.*
AG3	*Auditors rely on IT auditors mostly because they are the ones trained in how to check thoroughly the controls and their effectiveness.*
AG4	*Most of the audit evidence come in hard copy which bears the accounting general date stamp as valid documents.*
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 analyzing data, checking duplicates, complete data, etc..*

Source: Field data 2018

The auditors clearly rely on the use of auditing software such as ACL and IDEA to authenticate records in the system. Without documented procedures for the maintenance of authentic digital records in the system, it is not surprising that the auditors would use their own methods to determine the authentication of records in GABS.

4.3.2.5 Questionable authenticity of digital records in GABS

The third sub-question was: "Has the authenticity of accounting records in GABS ever been in question during audits?" The question was posed to both internal auditors (coded as IA) from the Department of Internal Audit and external auditors (coded as AG) from the Office of the Auditor General of Botswana. The responses are at Table 4.10.

Table 4.10: Instances of questionable records authenticity in GABS during audits

Participant	Response
IA1	*Yes. The audit of payroll and human resource management indicated that data is not completely clean. We have since recommended for data clean-up before we can conduct a comprehensive audit in some modules within GABS.*
IA2	*Yes, during auditing of payroll and HR. There were inconsistencies in 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 pay slips showed differently.*
IA4	*Yes, sometimes output from previous processes cannot be found on the system.*
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.*

AG2	*Yes, the schedule and the account (rate) not in agreement.*
AG3	*Yes. One employee from one ministry was able to make fake payments using GABS. If it was effective in its controls, it could have blocked that. If you discover something like this, you follow it up until you get satisfactory answers. Then the right measures, e.g. disciplinary action, will be taken against that culprit if wrong doing was done*
AG4	*No.*
AG5	*No. GABS is a very big system which has many modules, therefore I cannot say GABS was audited, instead I can say some modules were audited and data was acceptable*

Source: Field data 2018

The findings show that there have been instances where the authenticity of records in GABS has been questioned because of some unclean data and a mismatch between data in the database versus the one in paper records. Other participants were not aware of these instances as they happened in other ministries and departments and not where they worked. The participants, however, opine that GABS is a secure system if controls are followed and observed at all times.

4.3.2.6 Rejection of digital accounting records as evidence in the audit process

Another question posed to internal auditors and external auditors was: “Is there an instance where digital records have been rejected as evidence in the audit process and why?” The responses are presented in Table 4.11.

Table 4.11: Instances of rejected audit evidence and reasons for rejection

Participant	Response
IA1	*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. It has to be cleaned first. Yes, that has happened.*
IA2	*Not to my knowledge.*

IA3	*No*
IA4	*Yes, during overtime audits, data from GABS could not be confirmed from input processes.*
AG1	*Yes, when the records are incomplete.*
AG2	*Yes, where known factors (rates) were wrongly or not applied.*
AG3	*Yes, because they seemed to be having different figures as compared to hard copy done manually.*
AG4	*We do not get any digital records as evidence. We only get reports from GABS to audit then any supporting information it has be in hard copy.*
AG5	*No.*

Source: Field data 2018

The responses from the participants were mixed. Some auditors were not aware of records from the system being rejected based on their questionable authenticity. This does not come as a surprise in that at the time of data collection, IDEA, a system used by auditors at the OAGB had been down and unusable for some time and the auditors who were new had not used it. The more experienced auditors had conducted audits over the years (for example, payroll and overtime pay) and detected anomalies in the data from the system. The data were rejected on the basis that it was not reliable and authentic evidence to support the audit process.

4.3.2.7 GABS Functionalities for the creation of authentic digital accounting records

Apart from ICT professionals, internal auditors and Records Managers, external auditors (auditors from the Office of Auditor General Botswana) also took part in the study and responded to questions relating to procedures in place to maintain the authenticity of digital accounting records created and stored in GABS. The first sub-question was: “What functionalities does GABS have to ensure that it creates and maintains authentic reliable digital accounting records in the system?” The responses are reflected in Table 4.12.

Table 4.12: Computer system controls for securing digital records authenticity: auditors

Participant	Response
AG1	*Database security, segregated duties, data integrity checks, authorisations for transactions, physical security for servers, documented input procedures and automated processing of calculations. The system can capture and maintain records if fully utilised.*
AG2	*Categorises information per predetermined accounts. Once captured, information is stored as read only. No one can change it, except when need arises and only those authorized effect changes can do the same.*
AG3	*Still questionable, as fraud can still be seen in GABS. Controls in GABS I would say, are not that protected since it's easy for the users to fiddle with its inscription and do crime. Employees still being able to make transactions that under normal circumstances should be rejected by the system, being able to bypass certain fields.* *If controls can be fiddled with; obviously it means they are weak. Just like when you try to enter a building using your thumb as your code, it should not open the door for you if you don't work there.* *Because an outsider can be able to fiddle with data there to amend figures, it would give an audit opinion that would be untrue and unfair.*
AG4	*Accessibility by use of password at different levels.*
AG5	*I think data stored can only be read. I think segregation and the system do not allow any data manipulation along the processing path. If there is any error, the person on the next line in segregation cannot fix error.* *With segregation, for example, one person cannot initiate a payment, and authorise it in the system.* *If there is any error, say maybe in a transaction, the transaction cannot be edited, instead it is cancelled and then a new transaction is done. Allowing editions to be done comes the risk of compromising the reliability of the data hence the need for a new transaction*

	Data should pass different levels of review when processed so that at the end, accurate and reliable record can be kept or outputted. In addition, the flow of data from the time is captured all the way to the output and storage

Source: Field data 2018

The system analysis of the GABS database shows that it is a secure database. The system relies on both general information technology controls and system application controls to secure records in the system. The segregation of duties also ensures that no one officer can undertake many duties in the system and this is for purposes of protecting data in the system. The responses from ICT professionals on available computer system controls for securing the authenticity of records in GABS are presented in Table 4.13

Table 4.13: Computer system controls for securing digital records authenticity: ICT professionals

Participant	Response
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 validation of record before 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 user 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 HCM Oracle system.* *Creation of records is centralised, e.g. to create a company profile authority is sought from MFDP and personal data is extracted from HCM Oracle system.*
ICT3	*-Usernames and password 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/spent 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 same invoice number more than once.* *-All transactions created and validated cannot be deleted, they are rather cancelled to keep 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 supplier* *-The system can only be accessed by those in Government Data Network.*

Source: Field data 2018

GABS use general IT and system application controls to support the creation and maintenance of records authenticity in the system. Rogers (2015) refers to them as technical and social indicators of records authenticity.

4.3.2.8 Factors required for digital records to be acceptable in the audit process

One of the sub-questions was about the requisite factors that need to be in place for digital records to be acceptable in the audit process. It was posed to auditors. Their responses are presented at Table 4.14.

Table 4.14: Factors required for acceptance of digital records in the audit process: auditors

Participant	Response
AG1	*Auditors should be present when the data is extracted.*

	The data should be from the production environment, not other instances of the database.
AG2	*The records have to be correct and complete.*
AG3	*The policies should be in place together with frequent checklist reports to see whether controls always monitored are working effectively.*
AG4	*It should be signed and stamped with the Accountant General stamp that it is a correct copy. Most of the work we do as financial auditor we get reports from GABS in form of statements and votes ledgers. These reports give us information about transaction during the year and we do not rely on such reports so we do audits by checking such reports against accounting records such as payment vouchers which are hard copies; then when we will know whether the statement shows a true and fair view of what was happening.*
AG5	*The records have to be produced from the system in the presence of auditors. This is to make sure that they would not be manipulated in anyway.*

Source: Field data 2018

External auditors were also asked to describe the financial audit process they follow when undertaking an audit system such as GABS. A summary of the audit process is presented in Figure 4.3.

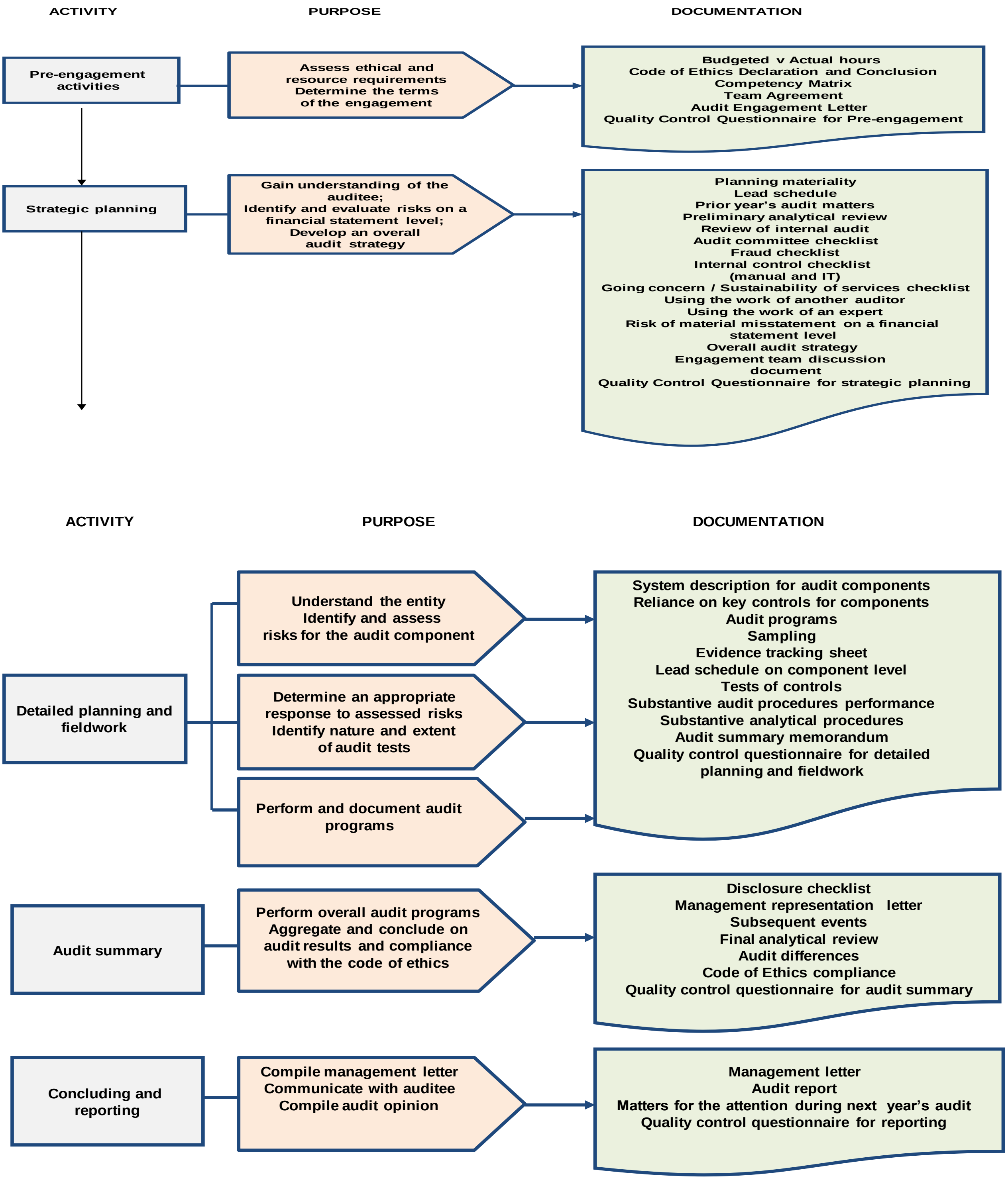

ACTIVITY
PURPOSE
DOCUMENTATION
Pre-engagement activities
Assess ethical and resource requirements Determine the terms of the engagement
Budgeted v Actual hours
Code of Ethics Declaration and Conclusion
Competency Matrix
Team Agreement
Audit Engagement Letter
Quality Control Questionnaire for Pre-engagement
Strategic planning
Gain understanding of the auditee; Identify and evaluate risks on a financial statement level; Develop an overall audit strategy
Planning materiality
Lead schedule
Prior year's audit matters
Preliminary analytical review
Review of internal audit
Audit committee checklist
Fraud checklist
Internal control checklist (manual and IT)
Going concern / Sustainability of services checklist
Using the work of another auditor
Using the work of an expert
Risk of material misstatement on a financial statement level
Overall audit strategy
Engagement team discussion document
Quality Control Questionnaire for strategic planning
ACTIVITY
PURPOSE
DOCUMENTATION
Detailed planning and fieldwork
Understand the entity Identify and assess risks for the audit component
Determine an appropriate response to assessed risks Identify nature and extent of audit tests
Perform and document audit programs
System description for audit components
Reliance on key controls for components
Audit programs
Sampling
Evidence tracking sheet
Lead schedule on component level
Tests of controls
Substantive audit procedures performance
Substantive analytical procedures
Audit summary memorandum
Quality control questionnaire for detailed planning and fieldwork
Audit summary
Perform overall audit programs Aggregate and conclude on audit results and compliance with the code of ethics
Disclosure checklist
Management representation letter
Subsequent events
Final analytical review
Audit differences
Code of Ethics compliance
Quality control questionnaire for audit summary
Concluding and reporting
Compile management letter Communicate with auditee Compile audit opinion
Management letter
Audit report
Matters for the attention during next year's audit
Quality control questionnaire for reporting

Figure 4.3: Auditor General of Botswana Audit Process

The audit process depicted is actually a procedure for undertaking a financial statement audit as adopted by the Office of the Auditor General of Botswana. The process is performed in stages such as pre-engagement activities, strategic planning, detailed planning and fieldwork, audit summary, and concluding and reporting. A closer look at the audit process shows that various pieces of documentation (records) are central in the process across all the stages. Data obtained from interviews with auditors indicate that analytical procedures are paramount when auditing in a digital environment. It is when there are issues or dissatisfaction with the findings from analytical procedures that substantive procedures are normally undertaken.

4.3.3 Skills and Competencies needed for the Authentication of Digital Records

The third objective of the study was to establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate/establish the authenticity and reliability of digital records created and stored in GABS. Several questions were posed and the first sought skills and competencies needed by records management personnel, ICT specialists and auditors to establish the authenticity of digital accounting records.

4.3.3.1 Skills and competencies needed by records managers

The records management professionals taking part in the study listed the following as skills and competencies needed to establish the authenticity of digital accounting records created and stored in GABS:

- Knowledge of digital preservation and computing skills
- Electronic records management
- Enterprise content management
- Legal aspect of information
- Analytical and planning skills
- Metadata and auditing
- Effective communication and consensus building skills

- Appreciation of secure digital signatures platforms
- Security and privacy control

4.3.3.2 Skills and competencies needed by ICT specialists

The ICT specialists indicated that in order to establish the authenticity of digital accounting records created and stored in GABS, the following skills and competencies are a basic requirement:

- System design
- Business process analysis
- Business rules
- Data analytics
- Computer forensics and security
- Database administration.
- IT certification (information systems auditor)
- IT security-related technical competencies
- Implementation of user roles and individual logging credential

ICT specialists need the cited skills in order to continue to stay abreast of developments in ICT. That is why some of the auditors undergo information technology security training while others get some training as information systems auditors. Continuous capacity building of the ICT specialists is a way of building skills and competencies required to secure ICT assets, including records and information in the system database.

4.3.3.3 Skills and competencies needed by auditors

It emerged from the findings that for auditors to effectively audit in a digital environment, ICT skills and competencies are a requirement. For them to establish the authenticity of digital records created and stored within GABS, they need to possess the following skills and competencies:

- Data analytics
- Business rules and business process analysis
- Knowledge of and the use of CAATs
- An understanding of system design and development
- Information system audit expertise
- Monitoring and evaluation
- Training on GABS as a system
- Presentation and creative skills

The auditors indicated that they needed skills and competencies to enable them to undertake audit assignments in a digital environment. During interviews, they opined that GABS was being upgraded and will have new features, which are not familiar to them. The various skills and competencies as indicated would really help them to conduct audits in a thorough and confident manner, something that is demanded from them as professionals in the field of auditing

4.3.3.4 Inadequate skills and competencies for establishing records authenticity

The second sub-question asked the participants (auditors, Records Management Professionals and ICT specialists) to state the impact of a lack of technical skills and competencies cited in the endeavour to establish the authenticity of digital accounting records created and stored in GABS. The responses of the auditors are presented in Table 4.15.

Table 4.15: Impact of inadequate competencies and skills of auditors

Participant	Participant response
IA1	*Compromised quality reports that do not improve the operations of the organisations. This could result in so many errors and even fraud committed in*

	GABS and go undetected for long. Delayed audit reports due to inadequate analytical skills.
IA2	*It would not be easy to establish the authenticity of data and transaction in the system. Fraudulent activities on transaction and data manipulation would not be easily identified. Government would lose a lot of money and officers who process transactions would take advantage of that to misuse government funds.*
IA3	*- Failure to interpret results* *- Failure to capture correct information*
IA4	*Unreliable audit findings with no value. Part of the definition of internal auditing is about adding value and improving the organisation's operation using systematic approaches to evaluate and improve effectiveness of risk management, controls and governance for decision-making. Using unreliable data is more like distorting the risk management process and accountability especially if COSO is the selected risk management model.* *In our case, we use COSO for risk management, which means Control Activities and Risk Assessment components of COSO are not a true reflection of some of the business processes within GABS environment. One evident deficiency can be realised in segregation of duties where an authorising officer can authorise at all levels enabling them to be able to complete a transaction with the aid of a preparing officer. The result of this was that one officer previously paid overtime more than basic salaries to some officers without detection for more than two years, a clear violation of remuneration policies.*
AG1	*Inadequate analysis of the data that has been collected which can lead to wrong conclusions.*
AG2	*Risk of issuing a contradictory audit opinion.*
AG3	*There will be reports that are not communicating to stakeholders on how government money was spent, and fraud can just happen in front of their eyes.*
AG4	*Irregularities may not be picked up because the auditor would not have had access to some information because if accountants are the ones who are used to provide*

	the reports, they may choose to omit some reports which they know would reflect some irregularities.
AG5	*It could lead to unreliable evidence/records that in turn could lead to false findings. False audit findings when reported have negative effects on the side of the office as people will question the integrity of the auditing institution*

Source: Field data 2018

The findings of the study pointed to the fact that any deficiencies in the competencies and skills needed by auditors to audit in the digital environment were bound to negatively affect the audit process. Incapacitated auditors would not be able to authenticate digital records in GABS and possible fraud would be undetected. If it so happens that audit reports are issued, they may be based on unreliable information and the audit opinions offered may not present the true state of affairs of financial statements.

When the question of the impact of inadequate competencies and skills needed by Records Managers would be on their abilities to authenticate digital records, they responded as shown in Table 4.16.

Table 4.16: Inadequate ICT competencies and skills for records management professionals

Participant	Participant response
RM1	*Usability and preservation might be adversely affected, thereby undermining the credibility or authenticity of digital records when the call to ascertain is made.* *Legal and technical assistance would be expensive to attain.* *Weakened capacity for ascertaining the authenticity of digital records.* *Reduced or no access to such records to ascertain their authenticity.* *Compromised or intellectual control of ascertaining the authenticity of digital records. Public distrust is imminent from digital records loss.* *Inability to provide the necessary guidance and direction on digital records.*
RM2	*It would be not easy to identify and authenticate of digital records.*

RM3	*Loss of suites in case of litigation.*
RM4	*Authenticating, accessing, maintaining, creating, even disposition of such records will be compromised.*
RM5	*Tempering with information or records is a critical step towards committing fraud, so lack of knowledge and skills about electronic systems results in mismanagement and leaves a room for exploitation by fraudsters.*
RM6	*They would not be able to design and use the systems as well as manage the digital records. They will not be able to know the authenticity of the records if they have the skills.*
RM7	*Lack of skills means one will not be able to use the systems in any way and authentication of records will not be ascertained*

Source: Field data 2018

Records management professionals lamented that without requisite ICT skills and competencies, they would not be able to competently manage digital records. The result would be that records under their care may be found wanting if they were to be used as evidence to support litigation. ICT specialists were asked about the impact of inadequate technical competencies and skills would have on their ability to authenticate digital records. They responded as tabulated in Table 4.17.

Table 4.17: Inadequate competencies and skills for ICT specialists

Participant	Participant response
ICT1	*Obviously, the system security will be compromised.*
ICT2	*There is likelihood of making mistakes or accidentally deleting data by overriding functions if one does not know the impact of such actions/ knowledge. This may cause data loss or corruption.*
ICT3	*Mistakes that can compromise data quality data in the system can happen. Information leakage, i.e. unauthorized personnel may have access to vital information.*

Source: Field data 2018

ICT specialists need to have competencies to enable them to execute their duties. The operation and success of information systems rests with ICT specialists. The findings showed that the ICT specialists were generally capacitated with ICT skills.

4.3.4 The Management of Authentic Digital Records

The fourth objective of the study sought to determine how digital records created and stored through GABS are managed as authentic and reliable to support audit processes in the public sector of Botswana. Several sub-questions were asked to participants that included MFED Records Managers, financial records management personnel at MFED RMU, users of GABS at the AGD and ICT specialists in the same department.

4.3.4.1 System analysis of GABS functional requirements

It was not possible to get hold of the system functional requirements, but the researcher garnered them from interview responses. These were confirmed by available documentary evidence. The analysis showed that GABS is an open system, hence its ability to interface with other business systems in the public sector of Botswana as well as banks. The interface is mainly for payment purposes. An analysis of GABS revealed that the system mainly comprised the following core modules:

- **Main Accounting System (MAS)**: It caters for the needs of the accounting functions performed at the AGD. It covers functions such as:
  a. data capturing of payments, receipts and journal vouchers
  b. preparation of payments and cheque printing
  c. reconciliation of bank accounts
  d. reconciliation of remittance accounts
  e. monthly and annual accounts processing.

- **Budget Administration Module (BAM)**: It caters for the needs of the budgetary process of the Government of Botswana and encompasses the total budgeting cycle of both development and recurrent budget for expenditure and revenue. The following major functions are covered in the module:
  a. Preparation of annual ceilings (constraints)
  b. Preparation of budget estimates at various levels (department, ministry) using work sheets
  c. Issuing of general warrants, finance warrants, withdrawal warrants, departmental warrants, virements, letters of authority, using dossier processes

- **Common Ministry/Votes Ledger Module (VLM):** It caters for the daily processes of budgeting and accounting for government ministries and departments. The following processes are covered:
  a. Procurement (quotations, purchase orders, receipting)
  b. Payment processing
  c. Revenue receipting and depositing receipts
  d. Air, rail and road warrants
  e. Repayment of unused travel and upkeep funds from official trips (travel imprest and retirement processes)
  f. Votes ledgers
  g. Request for finance, withdrawal and departmental warrants, and letters of authority
  h. Payments and dossier approvals
  i. Various reports

- **Revenue Office Data Module (RODM)**: It caters for the needs of revenue offices countrywide and it integrates with the MAS. The following major functions are covered:
  a. Processing of payments
  b. Processing of receipts
  c. Daily/monthly cash control reports

d. Treasury cashiers/sub-cashiers, cash, issues and receipt procedures
e. Cash accounts reconciliation
f. Bank accounts reconciliation

- **Agencies Module**: It maintains the Mine Workers Fund and Guardian Fund. It is integrated with MAS for payment purposes and covers:
  a. Payments
  b. Maintenance of ledgers
  c. Annual statements

- **Public Debt Servicing Module (PDSM)**: It caters for the needs of the Public Debt Servicing Unit (PDSU) of the Budget Administration Division of the MFED. The unit manages all external and domestic loans and covers:
  a. Loan schedule preparation and maintenance
  b. Receipts
  c. Payments
  d. Loans ledger maintenance
  e. Annual statements

- **Cash Flow Module (CFM)**: This module takes care of the needs of the Cash Flow Unit in the Budget Administration. The module draws data from various modules and generates reports.

- **Interfaces**: GABS is a critical system that caters for all government departments. This module caters for interfaces with various business systems across government. The system is designed to interface with interfacing requirements:
  a. Payments interface
  b. Receipts interface
  c. Journal voucher interface

GABS has the functionality to interface with other business systems that have modules for payment for services, issuance of receipts and generation of journals. These are:

a. Taxpayer Management System (TMS): payments interface

b. Value Added Tax System (BIVATS): payments interface

c. Central Medical Stores System (CMS): payments interface

d. Vehicle Registration and Licensing System (VRLS): receipts interface

e. Drivers Licensing System (DLS): receipts interface

f. Social Benefits and Reconciliation System: payments

g. Government Payroll, Pensions and Passage System (GPPPS): payments and receipts

GABS also interface with the Digital Imaging System (DIS) of the AGD for purposes of scanning and digitising documents to store accountable documents. The scanning of the documents is done through the DIS and then these are accessed through GABS. After this, these are displaced to users through the interface if there is a need. The design of the system caters for future business systems that have standard payments and receipts functions.

4.3.4.2 Types of records created and stored in GABS

The first question enquired about specific accounting records created and stored in the system. The findings revealed that records such as journals, receipts, vouchers, financial reports and invoices. A record of all companies and suppliers that do business with government are created and stored in the system in the form of a company profile. A company’s profile is first captured onto the system so that it can be paid for services rendered. Many more records are imported from other systems that have an interface with GABS. The digital accounting records in the system are actually categorised (modules) in accordance with the different transactions and these are:

a. Payables

-Invoice register

-Invoice batches

-Expenditure reports

-Payment registers

-Payment details to suppliers

-Outstanding imprest payments

-Listing reports

b. Receivables

-Auction reports

-Receipts from revenue

-Advance overpayments

-Police fines

-Deduction of salary overpayments

c. Budget

-Commitment and expenditure

d. After spending

-Estimated budgeted against collected revenue

-Recurrent expenditure – budget actual expenditure

-Development votes – budget against actual expenditure

4.3.4.3 The capture of accounting records into GABS

The second question asked whether digital accounting records were directly captured onto GABS or scanned onto the system. Participants indicated that for accounting records to exist in the system, they are directly captured onto the system while others are imported into the system from other systems that interface with GABS. Examples of the said systems have been presented in section 4.3.4.5. These systems are from other government bodies as well as trade unions. Other records are imported from banking systems and uploaded onto GABS. They further indicated that the system does not allow records to be scanned onto the system.

4.3.4.4 Retention and disposal of records in GABS

The third sub-question asked whether records retention schedules were to regulate digital records in GABS and whether records retention periods have been configured into GABS, bearing in mind that the AGD has issued Financial Instructions and Procedures that specify records retention periods for specific accounting records as part of their management over time. Participating Records Managers at both BNARS and the MFED responded as presented in Table 4.18.

Table 4.18: Existence of records retention schedule to regulate disposal of records

Participant	Response
RM1	*Not necessarily on digital records but a generic guideline on conventional records. Assumingly, this is in part, because of lack of capacity to develop and implement disposal guidelines for the same.*
RM2	*BNARS has issues with Generic Records and Retention Schedule for common records in the public sector.*
RM3	*No. However, the e-government office, a government department, is working on producing such, in conjunction with BNARS.*
RM4	*Currently, we are using the generic disposal and retention schedule, and also Financial Instructions as guiding tools.*
RM5	*There is a generic records retention schedule to guide on disposal decisions of finance records, the format of records does not necessarily affect the type, therefore disposal decisions will possibly still remain the same.*
RM6	*No. BNARS has not issued records disposal guidelines for management of digital records. The Financial Instructions and procedures regulate financial records in paper form.*
RM7	*There are no records disposal guidelines in place for managing digital records.*

	Off course, there are Financial Instructions and Procedures in place. They regulate the disposal of financial records (they are general procedures they are not specifically for digital or paper records).

Source: Field data 2018

GABS is a business system and therefore was not designed like a record-keeping system which is configured with records retention and disposal schedules. Records retention and disposal schedules aid the records appraisal process. Although the National Archives and Records Service's Records Management Procedures Manual calls for digital records to be systematically used throughout their lifecycle (BNARS 2009:42), there is no guidance on the management of records created in business systems. ICT specialists also responded to the question on records retention and disposal in GABS. The following are their responses as presented in Table 4.19.

Table 4.19: Records retention and disposal in GABS

Participant	Response
ICT1	*GABS still has old records from system commissioning and these need to be archived*
ICT2	*I am not sure*
ICT3	*There are no records retention and disposal periods set up in GABS. The system will not dispose any data by itself*

Source: Field data 2018

According to the Ministry of Transport and Communication Newsletter (2017), GABS does not have archiving capabilities and consumes a lot of data storage because of a lack of archiving and warehousing. As a result, "data from as far as the year 2003 is stored which renders the system slow" (Ministry of Transport and Communication Newsletter (2017:7).

4.3.4.5 Integration of GABS with other information systems

Participants were also asked whether GABS was integrated with other information systems (e.g. a digital records management system). A review of documentary evidence indicates that GABS provides an integrated set of business solutions that allows the Government of Botswana to manage budgets, record revenue collections, expenditure and control spending. GABS is integrated with some business systems in some government ministries and departments. The system has not been interfaced with an Enterprise Content Management system or an EDRMS, although it has capability. It has been interfaced with the following business systems:

- Human Capital System, which is used to manage personnel records of government employees. Its custodian is the Directorate of Public Service Management (DPSM), within the Ministry of Presidential Affairs, Governance and Public Administration.
- National Identity Registration System (Omang Identification System), which is used for the management of the registration process of citizens of Botswana.
- Vehicle Registration and Licensing System (VRLS), which is used for managing processes related to vehicle registration. Its custodian is the Department of Road Transport and Safety (DRTS) within the Ministry of Transport and Communications.
- Driver Licensing System (DLS), which is used for drivers' licensing and management. Its custodian is the DRTS.
- Central Medical Stores System (CMS), which is used for the management of centralised health care medicines before they are distributed to health facilities across the country.
- Government Payroll, Pensions and Passages System (GPPPS) whose custodian is AGD. The following functions are performed by the system and produce digital records:
  a. Employee data maintenance
  b. Data capture of payments and deduction elements
  c. Downloading data from third parties
  d. Payroll processing
  e. Cheque printing
  f. Electronic Funds Transfer to Bank of Botswana
  g. Payroll Bank Account reconciliation

h. Tax forms processing
i. Payroll processing for gratuities and pensions

- Value Added Tax System, which is used to manage VAT. Its custodian is the Botswana Unified Revenue Service (BURS).
- Taxpayer Management System (TMS), which is used to manage tax processes. Its custodian is Botswana Unified Revenue Service.
- Social Benefits and Reconciliation System, which is used for the payment of old-age pensions. Its custodian is the Department of Social Services.
- Supplies Warehousing and Inventory Management System (SWIMS).
- Development Projects Monitoring System, which is used for monitoring all development projects implementation (both physical and financial progress across government).
- Digital Imaging System (DIS), which is used for scanning, digitising and storing accountable documents. Its custodian is the AGD.
- Banking Integrated Settlement System (RTGS).
- Immigration and Citizen System (ICS).
- Ministry Investment, Trade and Industry’s Management Information System (MTIMIS), which computerised its core mandate inclusive of trade licensing, issuance of rebate certificates and export/import permits and registration, investigation and resolution of consumer complaints, amongst others.
- Fleet Tracking and Maintenance Management System (FTMMS), which is used for the tracking of the entire government fleet. Its custodian is the Central Transport Organisation, a department within the Ministry of Transport and Communications.
- Government Bookshop Online System (GPPS), which is used to transact publication orders and sale of government publications. Its custodian is the Department of Printing and Publishing Services.

In addition, findings from documentary analysis indicates that some information was capable of being integrated with GABS but had not been integrated at the time the study was conducted. These are:

- Student Loan Information System (SLMS), which is used to manage tertiary student financing and recovery of disbursed student loans. Its custodian is the Department of Tertiary Education Financing within the Ministry of Tertiary Education and Research.
- Court Records Management System, which computerised court management processes. Its custodian is the Department of Administration of Justice. It has been implemented in the High Courts and Magistrates' Court across the country.

4.4 Study Recommendations

This section presents recommendations geared towards the resolution of the research problem. They are presented in the section that follow.

4.4.1 Recommendations by Records Management Personnel

Records management personnel were requested to offer recommendations on the study as a whole and their responses are presented in Table 4.20.

Table 4.20: Recommendations by records management personnel

Participant	Response
RM1	*-Instigate a public sector-wide skills gap on the management of digital records among the Records Managers and Archivists.* *-Establish the current situation to inform the development of an electronic records management strategy to be implemented and monitored over time.* *-Development of paper to digital transition guidelines in the public sector.* *-BNARS to instigate a training needs analysis and skill gaps research on the same.* *-Stakeholders should have a working synergy to promote and complement efforts to create and maintain authentic digital records. BNARS to fastback the development*

	and implementation of the digital records strategy through a robust engagement of all stakeholders as part of an integral part of a deliberate strategic management of records, e.g. below. *-Strengthen the legislative framework by amending it so that it properly regulates the management of digital records that are authentic and can be reliable to conduct government business* *-Standardise the management of digital records in the public sector.* *-Establish an inter-ministerial/sector national standing committee that would provide to:* *-Promote deliberate continuous dialogue, engagement and empowerment of records managers on public sector digital records management issues through workshops, conferences, seminars and benchmarking visits among others for international best practices among those who have made strides on management of digital records.* *-Develop and maintain laws, regulations and standards for digital records sufficient to cover their definition, creation, capture, use, preservation and disposal as well as resources to realize proper implementation.* *-Use digital signatures to safeguard the authenticity of records in government information systems, GABS included.*
RM2	*-BNARS should provide direction and guidance in the creation, use, maintenance & disposal of digital records.* *-A strong legal framework should exist to guide proper management of digital records* *-Responsible staff should be trained on digital records management* *-Develop standardised policies and guidelines on digital records management* *-Cross-sectional approach: Records managers, legal practitioners, IT and e-gov leaders should work should collaborate in efforts to ensure the creation and maintenance of authentic and reliable digital records*
RM3	*Constant upgrade to the latest version, if there are any, in order to preserve records in the system. Also conduct refresher courses for users of the system*

RM4	*Records manager must be trained in financial records, ISO to be auditors, equipped with electronic records management*
RM5	*Stakeholders (Government, DIT, Department of Information and Broadcasting, BOCRA, High Court) should come together and deliberate on issues of Authenticity and related matters. Professionals are encouraged to research and study as well as benchmark from the best on issues of digital preservation. The developed countries are advanced on various issues or topics about the profession are readily available on the internet.*
RM6	*The records managers and BNARS were not involved in the development of the GABS system. Records managers do not man the records created in the system, hence their creation and maintenance are in the hands of accounts personnel. They only manage the paper records. It is crucial for Records Managers to be involved in the design and implementation of records system.* *BNARS as the overseer should also be visible to ensure that all records management systems are developed through their involvement since we are going electronic, including developing guidelines on management of digital records and emphasise compliance.*
RM7	*Records Managers should be included as advisers on the management of records in GABS.* *BNARS should also change their focus now from manual records to digital records. That is developing guidelines that govern the management of digital records.*

Source: Field data 2018

4.4.2 Recommendations by Auditors

Auditors were also asked to offer recommendations for ensuring that e-government information systems such as GABS create and maintain authentic reliable digital records. Their responses are presented at Table 4.21.

Table 4.21: Study recommendations by auditors

Participant	**Response**
IA1	*1. Data cleanup* *2. Training of data capturers* *3. Segregation of roles within the system* *4. Authorisation of amendments* *5. Strengthening controls within the system* *6. Continuous on the job and skill development on ICTs*
IA2	*Internal controls (application controls) and monitoring of transactions need to be improved. Starting from the designing of systems all stakeholders should be involved to ensure that the system has adequate, effective and efficient internal controls. After implementation of the system, system controls should be reviewed to ascertain the effectiveness. Monitoring of transactions can be done by generating weekly or monthly reports from the system to confirm if those reports are reliable and to check inconsistencies.*
IA3	*During the preliminary stage in the audit process, auditors should request manual files for sampling so that manual data could be compared with digital records.*
IA4	*The system should have audit trails in place and proper data storage procedures used.* *Internal auditors should be trained more on Internal Audit processes and techniques as they have accounting qualifications not internal audit ones. Capacitate internal auditors so that they are COBIT certified, Oracle certified and ACL certified.*
AG1	*Authorisations for all transactions, and all the transactions should be performed on the system for efficient tracking.*
AG3	*Proper and relevant training to programmers in order to produce what is communicative to auditors.*

AG4	*Auditee information is fine what is need is more training on side of auditors so that they would know the system very well.*
AG5	*There should be no or very minimum human interference in the processing of records except maybe at capturing stage only.*

Source: Field data 2018

4.4.3 Recommendations by ICT Professionals

ICT professionals were also requested to make recommendations for the study as a whole and the following were put forward:

- The disaster contingency site should be far enough from the production system (e.g. in a different city).
- A data warehouse should be built to house old records that currently sit in the system.
- Implementation of technology solutions to monitor activities of database administrators and system administrators.

4.5 Summary

This chapter presented the data collected through interviews, documentary review and system analysis. The summarised findings are organised in accordance with the study objectives.

4.5.1 The Legislative Framework for Digital Records Management

- The main legislation regulating public archives and records management is weak on digital records management.
- Some of the secondary legislation on records management, especially as it pertains to the creation of authentic reliable digital records, is available and fairly strong.
- Digital records are admissible in court proceedings as evidence.
- There is little awareness about legislation affecting records management in general and digital records management in particular.

- Legislation relating to public finance management and auditing is generally strong, but weak on guiding the management of digital accounting records that are authentic over time.

4.5.2 Procedures for the Maintenance of Authentic Digital Accounting Records

- Access control
- System audit trail to track user access and changes to record records and metadata
- Identity metadata
- Integrity metadata
- Segregation of duties
- Use of CAATs as financial data analytical tools
- Correct time system functionality

4.5.3 Skills and Competencies Needed by Auditors, ICT Specialists and Records Managers to Authenticate Digital Records

- Records management personnel need skills such as the following to authenticate digital records:
  - Knowledge of digital preservation and computing skills
  - Digital Records Management and Enterprise Content Management
  - Legal aspect of information
  - Analytical and planning skills
  - Metadata and auditing
  - Appreciation of secure digital signatures platforms, security and privacy control

- ICT professionals need the following skills and competencies:
  - System design; business process analysis and business rules
  - Data analytics; computer forensics and security
  - Digital records management

- Auditors need the following skills and competencies in order to authenticate digital records:
  - Data analytics, business rules and process
  - Knowledge of and the use of CAATs
  - An understanding of system design and development
  - Information system audit expertise; records management and creative skills

- Impact of lack of skills and competencies for establishing the authenticity of digital accounting records.
  - Compromised financial reports
  - Unspotted errors leading to fraud
  - Difficulties in establishing authenticity of data used for financial transactions
  - Unreliable audit findings
  - Wrong audit opinions
  - Compromised system security
  - Accidental deletion of records is a possibility

4.5.4. The Management of Authentic Digital Accounting Records

- Records in GABS are directly captured onto the system, imported from other systems and loaded onto the system.
- The digital accounting records in GABS are classified into different transactions.
- Records retention and disposal schedules for financial records are available, but are not configured into the system.
- Digital records preservation strategies such as refreshing, off-site storage, institutional disaster plan, technological preservation and migration to newer versions are used to preserve records in GABS.
- GABS is integrated with some public sector information systems.

The findings of the study showed that although GABS is a business system that was procured to manage financial transactions for government, it has good records management functionalities, although it is not really a record-keeping system. The next chapter interprets and discusses the findings of the study.

CHAPTER FIVE

INTEPRETATION AND DISCUSSION OF FINDINGS

5.1 Introduction

The previous chapter presented the findings of the study. This chapter interprets and discusses them. Taylor-Powel and Renner (2003:5) opine that data interpretation means attaching meaning and significance to data analysis. The findings are explained by using themes and their connections. In agreement, Neuman (2011:177) states that data interpretation involves assigning significant meaning to the findings. In data interpretation of the findings, the researcher draws inferences from the results of the research questions and the larger meaning of the results (Creswell 2009:152). That is why for Kothari (2004:344), data interpretation should be done with great care, objectively and within the correct theoretical perspective. In addition, Kothari (2004:345) points out that interpretation reinforces the "interaction between theoretical orientation and empirical observation" and that this is where the "opportunities for originality and creativity lie" in any research study.

The interpretation of the study findings is based on the research objectives, which were to:

1. analyse the legislative framework for the creation of authentic reliable digital records stored in GABS in support of audit processes in the public sector of Botswana
2. find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS
3. establish skills and competencies needed by auditors, ICT specialists and Records Managers to establish the authenticity and reliability of digital records created and stored in GABS
4. determine how digital records created and stored through GABS are managed and preserved as authentic and reliable to support audit processes in the public sector of Botswana

5. propose a framework for ensuring that authentic reliable records are created and stored in GABS to support audit processes in the public sector of Botswana.

5.2 Analysis of the Legislative Framework for Authentic Reliable Digital Records to Support Audit Processes

Archival diplomatics concerns itself with authenticity of records (McKemmish & Gilliland 2013:101). The International Council on Archives (1997:19) notes that "legislation governing many aspects of information creation, management, use and preservation has not kept pace with the rapid change in technology and archives legislation is no exception". Such has been the effect of digital technology on records management that it has gone against established traditional systems' norms of controlled production, validation and preservation of records and data (MacNeil & Gilliland-Swetland, 2005:21; Lauriault, Barbara, Taylor & Pulsifer 2007:140). Due to abrupt changes in digital technologies, archival legislation has often been left "weak," "outdated," "old and inconsistent" as ICA (1997:19) would say. This objective analysed Botswana's legislative framework to check whether it supports the creation of authentic digital records that can support audit processes in the public sector.

A strong legislative framework is necessary for the management and maintenance of authentic reliable digital records produced by information systems, as they transact organisational business. An information system such as GABS creates and stores accounting records that need to be availed as complete and accurate during the audit process. The records document payment processes, funds adjustment, allocation, expenditure, receipt and transfer of funds are done to conduct government business. The findings of this objective are presented and discussed according to the following sub-themes: laws, policies, standards and guidelines for promoting the creation and maintenance of authentic digital records and the role of BNARS in ensuring creation and maintenance of authentic public sector digital records.

5.2.1 Legislative Framework for Promoting Management of Authentic Digital Records

The findings of the study indicate that there are laws and guidelines that are meant to provide guidance about the management of authentic records in the public sector. These are the Constitution of Botswana, the National Archives and Records Services Act, the Electronic Records (Evidence) Act and its regulations, the Electronic Telecommunications Act and its regulations, the CCRCA of 2007 and the Criminal Procedure and Evidence Act. There are other laws such as the Public Audit Act and the Public Finance Management Act that regulate an audit of financial statements and the general management of government finances, respectively. They both have implications for the management of accounting records. There are also policies such as the National ICT Policy and the E-Government Strategy, which promote the use of ICTs in public service delivery and the adoption of e-government systems to transform the society of Botswana from a resource-based society into a knowledge-based society, respectively. The use of ICTs to transact public affairs result in digital records being created and as such, these policies impact on the management of digital records in the public sector.

5.2.1.1 Constitution of Botswana

The Constitution of Botswana (Government of Botswana 1966) lays the foundation for the management of financial resources for government ministries and departments. Although records management provides the basic layer for accountability (Ngoepe & Ngulube 2016:891), Isa (2009:148) observes that worldwide public sector organisations were yet to integrate records management and corporate governance. The Constitution prescribes in section 117 that all revenues or other moneys raised or received for the purposes of the conduct of business of the Government of Botswana should be paid into and from one Consolidated Fund. This section has records management implications. It implies that financial transactions (records) of revenue received and payable under any law for covering expenditure among departments should be retained as and when paid into or from the Consolidated Fund. Such financial records are to be retained for as long as needed as they would be needed for reference purposes and decision-making.

In section 124(1), (2), (3) and (5) of the Constitution empowers the Auditor General of Botswana to ensure government accountability on the use of financial resources by means of auditing financial statements of government entities annually. To facilitate that, the Auditor General should have unhindered access to financial records and books of accounts for auditing purposes and to report to Parliament through the Minister responsible for Finance. The Auditor General is constitutionally mandated to audit or inspect financial records emanating from the expenditure of government departments as they transact public services. Availability and completeness of such books, records, reports and other documents are a requirement for the audit process to succeed because, without such records, the performance of an audit becomes a futile exercise with no foundation for success. According to Ngoepe and Ngulube (2016:891), records are crucial in the audit process because more often than not, audit assignments are hampered by a lack of provision of supporting documentation when needed.

As the principal law of the land, the national constitution of Botswana does not have provisions for the creation of authentic records. That is not to be expected as a constitution usually provides a general framework for legal guidance. Explicit provisions for the creation of authentic records may be expected in actual statutory instruments.

5.2.1.2 National Archives and Records Services Act

Best practices in records management are underpinned by adequate evidence of compliance with the regulatory environment in the records of its activities, in the form of statutes, mandatory standard practice, codes of best practice and codes of conduct and ethics (Nengomasha 2009:83; Kalusopa 2011:228). According to Parer (2000:1),

> Records and archives legislation is an essential component of the wider legislative base of accountable and effective government. It provides the essential framework that enables a national records and archives service to operate with authority in its dealings with other agencies of the state.

Accordingly, the NARS Act is the principal law governing records management in the public sector of Botswana. The law established the archives and records management service in Botswana (Mbakile 2004:11; Keakopa 2006; Moloi 2009:109; Ramokate & Moatlhodi 2010:68), exercised through BNARS. The Act was enacted in 1978 and amended in 2007 to extend the meaning of a record to include a digital record.

Although the Act is the primary legislation for governing archives and records management practice (Parer 2000:1) in Botswana, it has been described as inadequate to regulate the management and preservation of digital records systems (Ngoepe & Keakopa 2011:155; Moatlhodi 2015:74). It does not provide guidance on the management of authentic reliable digital records in spite of e-government information systems, which, by their nature, produce digital records (Wamukoya & Mutula 2005a:68; Mnjama & Wamukoya 2007:277).

The Act is rather passive, and its amendment has not been helpful as it went as far as including the previously omitted digital record in its meaning of "record". It does not really provide guidance for the creation and maintenance of authentic digital records. According to Okello-Obura (2011:4), records and archives legislation forms part of a wider legislative platform for accountable and effective government. With its limitations, the Act provides a weak framework, contrary to the expectations that it should enable BNARS to operate with authority in its dealings with government ministries and departments over the management of records, including digital records.

It can be concluded that the National Archives and Records Services Act, which gives BNARS its archives and records management mandate, has the capacity to promote the creation and maintenance of authentic records in the sense of archival diplomatics. According to MacNeil (2007:534), records are the evidence of transactions performed. Secondly, archivists have an obligation to protect the integrity of such evidence. Lastly, it is their job to protect the integrity of evidence by protecting its impartiality. With the weaknesses inherent in national archival legislation, it is impossible to trust archival institutions to acquire digital records whose authenticity has not been established based on their custodial history. They must be subjected to tests of authenticity before they are ingested in archival custody (Cook 1986:7). With paper records, by virtue of being held in archival repositories, they were deemed authentic (MacNeil 2005:265). Even Jenkinson (1937:4) believes that archival documents "were authenticated by the fact of their official preservation."

The weakness of the national archival legislation also means that it is inadequate to guide the lifecycle management of records, especially digital records whose preservation starts at creation (Goh & Duranti 2012:3). It should also assign shared roles and responsibilities of the creator and the preserver along the entire life cycle of the records. Scholars such as Ngoepe and Keakopa (2011:155) and Ngoepe and Saurombe (2016:30) point out that archival legislation is weak and is unable to guide the management of digital records, not to mention their authenticity. To this end, Ngoepe and Saurombe (2016:30) further ask questions relating to the ability of the National Archives and Records Services Act (Government of Botswana 1978), as amended in 2007, and these relate to cloud-based records management of which records created and stored in GABS are implicated, as GABS is a web-based digital accounting system. They posed the following questions with reference to Part IV (1):

- Can the Minister declare a cloud as a suitable place for the storage of records?
- Does the Minister have the capacity to determine such suitability? What are the legal obligations of having such a declaration?
- Do the Minister and Director have the legal capacity to monitor the cloud and ascertain whether there are violations in the cloud?
- Can they charge those responsible for such violations?

At present, the Act is limited in that the law is not yet positioned to go that far. Part VI (17) provides for copies of records in the national archives or a place of deposit to be certified as true and authentic by the Director of BNARS or an officer designated as the custodian of public archives at the place of deposit where the records are kept. The authentication is to be done using BNARS's seal or the designated place of deposit's seal, and the records are to be admissible as evidence if the original record would have been admissible. For paper records, authentication by way of a seal on the record is done by using an office stamp. This stamp can also certify a copy of a public record as a true copy of the original, thereby ensuring the status and significance as the original. Lauriault et al. (2007:140) attest that authenticity is closely linked to the concept of trustworthiness, a reason why a record is deemed trusted enough to be admissible in any proceedings after it has been authenticated. With digital records, the provision of authenticating records using a seal is neither here nor there because currently, BNARS does not even have guidelines for managing public sector digital records, let alone guidelines on how to maintain digital records authentic. With reference to the aforementioned, Eastwood (1994:127) maintains that "the contingencies that endow authenticity are observable not in the document itself but in the procedures of creation, maintenance, and preservation."

Archival legislation that does not cover authenticity of records is not peculiar to Botswana only. Even in some developed countries, this situation remains. For example, in 2001, ICA's Committee on Archival Legal Matters conducted a survey among 13 countries, including Andorra, Australia, France, Germany, Italy, Lithuania, Mexico, Slovakia, South Africa, Sweden, United Kingdom and the United States. One of the questions was, "Does archival legislation in your country define 'authenticity,' reliability' or validity' in relation to records/ digital records?" (Gränström, Hornfeldt, Peterson, Mariana, Schäfer & Zwicker 2002:7). All the countries gave "no" as answer. The authors argue that the uniform answer was because archival legislation predated digital records.

5.2.1.3 Electronic Records (Evidence) Act and its regulations

Both social and technological developments in civilisations entail that laws that govern human action must also change, lest they be overtaken by time and become irrelevant (Piasecki 1995:54). As of April 2014, Botswana did not have a legal framework that facilitated and enabled the provision of digital services. The then available legislation tended to prohibit rather than promote the use of ICTs to provide services (Keetshabe 2015).

The Electronic Records (Evidence) Act was passed as law (Government of Botswana 2014a) to provide for the recognition of the authenticity of digital documents and admissibility of digital evidence (Keetshabe 2015). The Act also provides for the authentication of digital records in courts of law. The digital record as evidence carries the same weight as its paper counterpart and cannot be thrown out by the court on the basis of the fact that it is digital. According to MacNeil (2004:201), archival research seeking to identify requirements for assessing and maintaining the authenticity of digital records must deal with a number of questions and these are related to the issue of the context of such records. The questions are as follows:

- What constitute meaningful frames of relevance when it comes to investigating the authenticity of digital records?
- How much contextual knowledge is necessary to establish and assess their authenticity?
- How much context must be preserved to maintain that authenticity over time?

MacNeil (2004:201) goes further to propose contemporary archival diplomatics as one method of inquiry that can address the above questions. This is because archival diplomatics analyses aspects of digital records that should be considered in determining whether such records can be deemed to have authenticity. This determination is based on the manner of records, including the procedures governing the creation of records (MacNeil 2004:200; Duranti, Rogers & Sheppard 2010:99).

A document analysis of the Electronic Records (Evidence) Act (Government of Botswana 2014) at section 5(1) bars the rejection of digital records as evidence because they are digital, but it has to be proved that they are authentic. In section 5(4) the Act prescribes that when digital records are tendered to be admitted as evidence in proceedings, the burden is placed on the one tendering such evidence. Accordingly, Stanfield (2016:11) posits that real evidence should be able to speak for itself rather than rely on what someone else says about it. The same author puts across the view that normal digital documents fall within the category of evidence that speaks for itself. The admissibility of digital records as evidence because they have been authenticated then has to satisfy the following two criteria of the courts:

- Whether the digital record is relevant and has authorship, authenticity, correct operation and reliability has been established.
- Whether, according to the rules of evidence, the digital record has been collected and handled correctly.

The Electronic Records (Evidence) Act (Government of Botswana 2014) thus prescribes for the creation and maintenance of authentic digital records in line with principles of archival diplomatics as it relates to records authenticity. For example, it advocates for records to be declared authentic if the record was produced following a duly approved process that, in this case, refers to the information system producing such a record having been certified by BOCRA. Dahiya and Sangwan (2014:108) opine that the only useful evidence (record) is the one that has been proven authentic.

This piece of legislation is timely as the Government of Botswana has an e-government programme in place. Other than that, e-commerce is now a reality. According to Mnjama and Wamukoya (2007:281), it is of great importance to examine whether the government accepts digital records as evidence when assessing laws, policies and procedures. Makulilo (2016:132) observes that the admission of digital evidence presents challenges due to the unique nature of the digital technology, which has strained the common law rules of evidence, especially authenticity. Perhaps that is why Duranti et al. (2010:95) in their analysis of the Uniform Electronic Evidence Act of Canada opine that dealing with digital records is complex due to processes relating to their creation, use and storage. The authors conclude that due to changing technologies, it is not enough to account for the nature and characteristics of digital records by simple modifications to existing laws of evidence. Rather, the enactment should be a result of collaboration by various professionals such as records management, legal and law, and IT. Duranti et al. (2010:95) add that such a move would ensure that new rules are based on the body of knowledge of each profession, the findings of interdisciplinary research and existing records-related standards. It is the contention of the authors that:

> Rules would help the courts make accurate findings of fact, based on electronic records that are created in a reliable environment and preserved in an authentic form for as long as they might be needed, and would alleviate ongoing confusion about the admissibility and use of electronic records in litigation.

Therefore, these are important laws that are enacted. Especially those dealing with digital records as admissible evidence before the courts should be the result of collaborative efforts of the aforementioned disciplines. That way, the courts would be able to discern the authenticity and reliability of records produced in a digital environment far more easily than is currently the case. Researcher such as Duranti et al. (2010:99) opine that if proper rules governing the capabilities of digital records as evidence are to be developed and implemented successfully, there is a need for collaboration between archives and records management professionals, lawyers, notaries, judges, law enforcement officers and IT experts. All these bring together knowledge of the conceptual and methodological body of knowledge of diplomatics and digital forensics, and archival science should guide research in finding solutions to the challenges associated with admissibility of digital records as evidence in proceedings (Duranti et al. 2010:99).

5.2.1.4 Electronic Communications and Transactions Act

Contemporary communication systems across the globe have created a new economic and democratic landscape where societies have come close to each other and became integrated in the global economy through digital communications. This has been more of a revolution than an evolution and now the world has completely changed the way it operates, including in business dealings (Gereda 2003:264). Communications and transactions mediated through networks and computers are now a common feature in a business environment like between businesses. Business to government and business to employee e-commerce takes place online

(Australian Accounting Research Foundation 2002:5). E-commerce is risky so auditors of financial statements need to consider such risks when planning and performing an audit engagement. In the context of the Botswana public sector, auditors would require a sound legal framework to guide and support e-commerce transactions.

This study has revealed that national archival legislation does not provide for the creation and maintenance of authentic digital records. In a study among 13 countries that included both developed and developing countries, Gränström et al. (2002:7) found that those provisions were mostly present in legislation dealing with e-commerce in seven countries, while in six countries there was none. Botswana is player in the global economy and has a law that regulates e-commerce called the Electronic Communications and Transactions Act (Tafa 2016:1).

The ECT Act was enacted in 2014 to provide for the facilitation and regulation of digital communications and transactions, specifically to regulate digital commerce and digital signatures. In section 3(a) and (b), the ECT Act gives a legal recognition of both internal and external digital transactions, which produce digital records. Smedinghoff and McKenzie (2002:4) are of the view that the legal validity and enforceability of transactions conducted in a digital environment is an issue that needs to be addressed from the onset. Part of addressing issues around it includes a consideration of legal barriers that might arise as well as additional requirements related to enforceability that can be imposed because of the nature of the transaction, for instance, accept what this provision of the Act suggests is that as long as the requisite elements needed in such transactions are present and satisfied, such transactions should pass the bar, by the courts as legally valid and enforceable.

As long as foreign certificates or digital signatures conform to international standards, they are trusted to authenticate digital records in a similar way to local ones (Government of Botswana 2014b). Conformance to international standards enable the systems producing digital records to be secure and reliable. The UNCITRAL Model Law on Electronic Signatures (United Nations 2001:6) is one such international benchmark against which the ECT Act can be gauged. The UNCITRAL Model Law on Electronic Signatures indicates that:

> 1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
>
> (a) To the geographic location where the certificate is issued or the electronic signature created or used; or
>
> (b) To the geographic location of the place of business of the issuer or signatory.
>
> 2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.
>
> 3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability (United Nations 2001:6).

It is notable that the ECT Act adheres to this model law as section 31 of the Act prescribes that in determining the legal validity of the digital certificate or certificate, there should be no regard for the geographical location where the certificate was issued or digital signature created. The geographical location of the place of business of the issuer of the certificate or the signatory is also not an issue. Furthermore, the Act recognises that "a digital signature created or used outside Botswana shall have the same legal effect in Botswana as a digital signature created or used in Botswana if it offers a substantially equivalent level of reliability." Yet another authority on digital signatures with international stature is the European Directive on Electronic Signatures, which sets conditions necessary for the creation of digital signatures and certificates (European Commission 2015).

The Act also gives legal recognition to digital signatures and the admissibility and weight of digital communications (Government of Botswana 2014). Accordingly, the legislation gives a technologically neutral legal framework for the creation of digital signatures such that both paper and digital signatures carry the same weight in terms of their recognition for the authentication of records. This is in relation to the provisions on the Electronic Records (Evidence) Act such that in legal proceedings, the rules of evidence would not be applied to deny the admission of digital records because they emanated from digital communication. According to Keetshabe (2015), the ECT Act gives digital signatures the equivalence of handwritten ones. In Hungary, similar legislation known as the Electronic Signature Act also provides for the legal recognition of digital signatures and ensures that they are presumed to be admissible in court. They may not be challenged successfully based on the mere fact that they are in digital form (Blythe 2007:47). Security in digital transactions over the internet is a critical issue in the digital space, a reason why "both international and supranational organisations on governmental and business level have been trying to promote the use of digital signatures in the e-commerce and set forth a common legal framework for electronic authentication over the Internet" (Spyrelli 2002:2). Just like its Hungarian counterpart, the ECT Act was enacted to facilitate secure e-government transactions.

This Act also promotes a legal framework to support digital commercial practices, including the formation and conclusion of legal contracts through digital means as well as the recognition, promotion and implementation of information technologies, which facilitate e-commerce just like paper-based transactions. According to Keetshabe (2015), the Act serves as a legal framework to support digital commercial practices, including the formation and conclusion of legal contracts through digital means. E-commerce transactions produce digital records. The question that arises in the transactions is whether the resultant records can serve as undisputed evidence of the said transactions. Their authenticity thus comes into question. According to Nengomasha (2009:90), the challenge for digital records management is to ensure the preservation of digital records' authenticity.

In essence, this Act contains provisions that prescribe the creation and maintenance of records authenticity as in the archival diplomatics sense. It recognises digital signatures as a way of authenticating transactions arising from digital communications (Government of Botswana 2014). Digital communications produce digital records. According to Dumortier and Eynde (2002:1), a "digital signature technique allows authenticating digital information in a way that the origin of the information, as well as its integrity can be verified." Gränström et al. (2002:5) argue that authentication determines whether an item introduced as evidence in legal proceedings is authentic. Digital signatures and other methods such as timestamps, hash digests, passwords, randomly generated number, a biometric measurement, checksums and cyclic redundancy checks are used to establish the authenticity of digital records (Elliot 2007:2; Mir & Banday 2012:225; Tank et al. 2013).

Gränström et al. (2002:5) indicate that in order to ensure the authenticity of digital records, organisations should issue and implement policies and procedures for managing records. According to ISO 15489-1 (2016:8), the objective of the policies and procedures is to:

> Ensure the authenticity or records, organisations should implement and document policies and procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that records creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment."

For records to be accepted as authentic in archival diplomatics thinking, methods should be instituted that can ensure that the records are not manipulated, altered or falsified after their creation (Duranti & MacNeil 1996:55). By recognising digital signatures in commerce transacted through the networked environment, the ECT Act acknowledges that the authenticity of digital records can be ensured through the use of digital signatures (Lim 2003:183). Notably, this piece of legislation recognises the use of digital signatures to authenticate digital records in conformance with the provisions of Electronic Records (Evidence) Act.

5.2.1.5 Cybercrime and Computer Related Crimes Act

The advent of e-commerce has helped international trade with minimum investment of capital, enabling organisations to easily reach out to more customers and suppliers across the globe. This has come with cyber threats to digital systems, which transmit records and information used in online transactions (Shweta, Vikas & Naveen 2016:807). As a country, Botswana conducts its government operations using ICTs as is common in the digital age. The CCRCA was enacted to combat crimes committed with the aid of computers and through cyberspace (Government of Botswana 2007). This legislation recognises digital records, and its definition of a digital record is consistent with general definitions of digital records, for example, as in IRMT's Glossary of Terms (IRMT 2009:12-13). This legislation is very important for the creation and maintenance of authentic reliable digital records created and maintained in business information systems used to transact government business.

In the conduct of financial transactions through GABS, digital accounting records are created. In general terms, the CCRCA outlaws obtaining unauthorised access to computer systems and data and performing actions such as modifying or deleting it. According to the National Electronic Commerce Coordinating Council (NECCC) (2004:11), it is difficult to protect the authenticity of records in a digital environment, as the media are inherently unstable (Cloonan & Sanett 2002:71). They can be easily modified or deleted without anyone noticing and this can negatively affect digital records in the system in such a way that they lose their evidentiary value due to their administrative context not being maintained (State of Alaska 2009:5). This is the reason why the NECCC (2004:11) asserts that it is important for authentication technologies to be in place to regulate access to computer-based information systems. The said technologies should be able to protect the authenticity of digital records by ensuring that archival documents' identity can be established, and their integrity confirmed (Rogers 2016:20).

According to Rogers (2015:95), there are technical indicators of records authenticity that are the result of a work process or a state change in records (e.g. system metadata capturing date created and date modified). Alternatively, the technical indicators may be implemented by the technological (e.g. computer, networks) components of a records system and these are deployed to create, manage and control system access and security (Rogers 2015:95). Section 4 of the Act shows that a person will be guilty of an offence when he or she accesses a computer system or part of it without the permission to do so (Government of Botswana 2007). Access control can be used to the authenticity of digital records. It helps in ensuring that the source of a digital document or message is identified correctly (Shweta et al. 2016:808). According to NARA (2005), digital records are vulnerable to forgery and tamping. This provides grounds for access to computer-based information systems to be controlled in order to prevent possible tampering such as deletion, addition, alteration or modification of records.

In the context of this study, strong legislation is a necessity in order to promote the creation and sustenance of authentic digital accounting records. This piece of legislation has been gazetted for amendment in order to strengthen the fight against cybercrimes and other acts committed using computerised technologies. The proposed Cybercrime and Computer Related Crimes Bill carries stiffer penalties for crimes committed when compared with the Act currently in use (Government of Botswana 2017b). This is done for purposes of improved protection of information resources, including the authenticity of records. For example, gaining unauthorised access to a computer or computer system carries a penalty of P10 000, while in the proposed Act the amount is P20 000.

The United Nations (2004:48) underscores the importance of records in the accountability process by saying that systematically kept records not only help track transactions, but also provide a documentary trail of decisions taken, and this trail (records) can be used in court when particular decisions are contested. Okello-Obura (2012:3) rightly contends that without reliable records, accountability processes demanded of the government, civil society and the private sector cannot be satisfied. In addition, Palmer (2000:64) concludes that:

> Records management, accounting and auditing provide layers of control that are essential to ensure transparency, probity and integrity in financial management systems. Together, records management, accounting and auditing provide layers of control that are essential to ensure transparency, probity and integrity in financial management systems. Financial record keeping in particular needs records that provide the basis for accounting and introduce controls that protect essential audit trails to curb corruption and fraud. It is record keeping that gives form and substance

> to financial systems and provides the means by which financial decisions and transactions may be verified and reported.

Therefore, suffice to say that digital accounting records in GABS need a stable environment in order to continue to serve as evidence of transactions performed. However, a strong ICT infrastructure is also still inadequate. Legislation that influences archives and records management also needs to be in place to give force and effect to what needs to be done to keep digital records authentic and reliable to enable their acceptance in the audit process. This Act contains provisions that endeavour to protect the authenticity of records in computer-based information systems, GABS included. It outlaws interference with data through events such as damaging, deteriorating, deleting or modifying. It also makes it a crime to modify and destroy records in the system. Even an authorised user who unlawfully discloses their password or access code commits a crime and can be fined P10 000 and face a six-month prison term, or both, if found guilty (Government of Botswana 2007).

5.2.1.6 Criminal Procedure and Evidence Act

This piece of legislation in its current form does not recognise the admissibility of digital records as evidence in court. It was enacted with documentary evidence in mind. It provides procedure and evidence in criminal cases to provide for other matters related to such evidence and procedures (Government of Botswana 1939). Section 244 prescribes that for documentary evidence to be accepted as evidence by the courts, an officer entrusted with their custody should have managed the archival documents concerned. From time immemorial, archival documents kept in an archive were accepted as authentic because archival institutions were trusted with the ability to maintain the authenticity of records in their custody (Jenkinson 1937:11; Eastwood 1994:125; Duranti 2007:447). However, Cook (1986:7) challenged the notion that archival documents should be treated as authentic on the basis that they had not changed official study. The author added that there must be tests for indications of authenticity through studying records provenance and elements of their form (diplomatics).

Records can also be regarded as authentic because they were used to transact organisationally and thus served as the evidence of those transactions. Such kind of authenticity is recognised by archival diplomatics (InterPARES 2002:2). Jenkinson (1937:11) notes that the two features of archival science, being records impartiality and authenticity, derived from the fact they were drawn up and used in the course of administrative or executive transactions.

Lastly, the archival documents should have been certified as a true copy of the original in such a way that it carries the same evidential weight as the original copy, including methods of authentication. Duranti (2005:2) avers that "authentic records have force of proof and the ability to produce consequences from the date that is affixed to them (this becomes important with digital records)." In this context, authentication means declaring authenticity by way of affixing some sign like a digital signature to the document.

In its present form, the Criminal Procedure and Evidence Act cannot be used with respect to digital records. However, the digital age means that societies function in both the physical and digital medium. Digital gadgets such as computers, mobile phones, printers, iPods and digital cameras are commonly used. Just like the physical medium, the digital medium presents opportunities for the commission of crimes (Watney 2009:2). In that instance, perpetrators of such crimes need to be prosecuted and one of the parties to the proceedings may need information generated in digital form such as spreadsheets, emails, text messages, databases and traffic data as evidence to prove or disprove facts. Duranti (2010:101) acknowledges the challenges associated with computer-generated or -stored records such as their lack of stability of form and content, and the fact that they can be displayed on a variety of media, but that does not automatically make them inadmissible by the courts.

The assertion by Duranti about difficulties in managing digital records due to their storage media as well as lack of stable form and content point to the need to keep digital records authentic for them to be acceptable in the audit process. Generally, records management is implicit in many laws (Phiri 2016:74), let alone authenticity of records. Unfortunately, even in archival legislation, issues of records authenticity are not expressed adequately as shown by archival legislation in a study that compared archival laws of the United Kingdom, Singapore and Canada.

5.2.1.7 Public Audit Act

The financial audit process results in an audit opinion. According to David (2017:1), accounting information from public entities is crucial in advancing the governments' efforts to promote public democracy and development. The Public Audit Act (PAA) outlines the duties of the Auditor General of Botswana regarding an audit of public sector organisations. The auditing of financial statements from public bodies is annual and must be done in accordance with the provisions of the PFMA.

The audit process relies heavily on records. The close association between records management and auditing makes records management a crucial governance function, both explicitly and implicitly (Phiri 2016:148). In the PAA, requirements for record keeping are implied. Phiri (2016:74) observes that "an objective to improve governance, for example, through accountability can be worked upon to be an outcome for a record keeping programme." The process of auditing which calls for accountability, in this context of financial resources, is a subset of governance since records management requirements can be implicit in legislation (Phiri 2016:74), as in the PAA. Accountability for the use of state resources then becomes a priority of executives and records management professionals are challenged to plough through implicit legislation in order to build business cases for good governance with records management as a pivot. Wickman (2009:119) attests thus: "I imagine that not many governments really care whether or not they have improved recordkeeping. They may, though, care about a policy outcome of increased efficiency and accountability which recordkeeping enables."

The PAA prescribes that an audit of financial statements must conform to existing auditing standards, manuals or codes of ethics. In the Botswana public sector, such standards are the various standards issues by the International Auditing and Assurance Standards Board

(International Federation of Accountants 2015). The standards do not offer guidance on how to ensure the authenticity of records (audit evidence) consulted during the audit process, although they infer that audit evidence is central to the audit process. Ngoepe (2013:58) carried out an informetrics analysis of the general reports of the AGSA from 2005 to 2010, and the findings revealed that records management contributed to audit opinions.

5.2.1.8 Public Finance Management Act

The PFMA enables accounting officers in government ministries and departments to use allocated financial resources and account for their usage. The Office of the Auditor General of Botswana exercises a check of accountability through an annual audit of financial statements after their preparation by the AGD (Government of Botswana 2011b). A comparison of this legislation with its South African counterpart shows that it also prescribes accountability of allocated resources against the budget, revenue management, expenditure, assets and liabilities, its business activities, its financial results, and its financial position as at the end of the financial year (Ngoepe 2012:75). The financial audit process thus relies on the availability of records in order to give worthy audit opinions. In agreement, Willis (2005:90-94) indicates that records enable scrutiny of what was done and how (transparency), but also enable answers to be given when sought (accountability) and these two combine to facilitate the process of doing things in an agreed, documented and controlled manner (due process). The PFMA is therefore a crucial control mechanism in the financial audit process, which, as a legal instrument, has to be complied with, as its provisions are obligatory. The PFMA implicitly promotes the proper management of accounting records to facilitate the annual auditing of financial statements, but it does not provide guidelines of how that is to be done. In addition, it regulates auditing in both the digital and physical environment, and it does not say anything about the need to create and maintain authentic records.

5.2.1.9 Summary of the legislative and policy framework

The legislative framework for the management of digital financial and accounting records in Botswana's public sector, including their authentication, is available. At the apex is the Constitution of Botswana, which makes provision for the establishment of the OAG that undertakes a financial audit of government financial statements (Government of Botswana 1966). The National ICT Policy and the E-Government Strategy are national policies that promote the use of ICTs in the delivery of services. The two complement each other to support e-government services in the public sector (Government of Botswana 2011a; Moatlhodi 2015:43).

Laws such as the Public Audit Act and the Public Finance Management Act are instruments for ensuring that public sector bodies are accountable for the use of public monies entrusted with them (Mosweu & Ngoepe 2018:149). Other laws such as the Electronic Communications and Transactions Act, and the Electronic Records (Evidence) Act recognise the authentication of digital records using digital signatures. In addition, they make provisions for the admissibility of digital records as evidence in the law courts of Botswana (Government of Botswana 2014a; 2014b). These laws supplement the National Archives and Records Services Act that is the principal legislation that regulate public sector records management in Botswana (Government of Botswana 1978). Although the law recognises digital records as public assets, there are no guidelines to guide their management (Mosweu & Ngoepe 2018:152).

Apart from laws and policies, there are standards to guide both the audit process and the management of records. In terms of auditing, the Government of Botswana subscribes to the International Financial Reporting Standards issued and interpreted by the International Accounting Standards Board (Government of Botswana 2010). The standards specifically guide the auditing of financial statements and these are not covered as explicitly as in legislation (Mosweu & Ngoepe 2018:157). Lastly, as the entity entrusted with national public sector records management, BNARS has adopted best practices in records management in the form of ISO 15489-1 (2016), but this has not been formalised through adapting the standard to the local environment. According to Moatlhodi and Kalusopa (2016:9), and ISO 15489-1 (2016), among other tools, records management standards provide a framework for the development and implementation of a records management programmes.

5.3 Procedures for the Creation and Maintenance of Authentic Digital Records

The second objective of the study sought to find procedures used to maintain the authenticity of digital accounting records created and stored in GABS. The InterPARES (2002:5-7) Benchmark Requirements Supporting the Presumption of Authenticity of Digital Records was used as an evaluation tool for assessing records authenticity, and the findings revealed that GABS as a system 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

In essence, GABS as an information system produces digital records deemed as such by archival diplomatics. The records created through GABS qualify as records in terms of diplomatic analysis. The records creation includes the required persons such as the author, addressee and writer (InterPARES 2002:5; Hawkins 2006:3). This is attested by the system having all the InterPARES Benchmark Requirements Supporting the Presumption of Authenticity of Digital Records (InterPARES 2002). In essence, accounting records in GABS can be said to have identity and integrity and thus authenticity. A number of procedures are used to authenticate digital records in the system. They include those as stipulated by records management professionals, ICTs and auditors.

5.3.1 Procedures for Declaring Records Authenticity by Records Management Professionals

This study revealed that the management of digital records in Botswana in general and the AGD is still in an infant stage. This is because the records management professionals, through their responses, indicate that there are no procedures in place for ensuring that digital records remain authentic. These findings are like others in earlier studies that have also depicted limitations in public sector digital records management. A study by Moloi (2009:122) on readiness for digital records management in the public sector of Botswana revealed an absence of policy on digital records management, whose absence made it difficult to identify, maintain and preserve e-records. A lack of policy on digital records management suggests that procedures for the maintenance of authentic digital records would also be absent. Weaknesses in the management of digital records management have also been revealed by a study that compared the state of archival and records systems between Botswana and South Africa. The study found that the public sector in Botswana does not have the infrastructure to ingest digital records in their custody for permanent preservation (Ngoepe & Keakopa 2011:157). It would seem that the capacity to properly manage digital records is not limited to Botswana, as even the ESARBICA region has similar limitations in general terms (Keakopa 2010; Ngoepe & Keakopa 2011:157; Nkala, Ngulube & Mangena 2012:114; Ngoepe & Saurombe 2016:37-38).

5.3.1.1 Standards for creating authentic digital records

Organisations need to identify the regulatory environment that affects business activities and have them documented through policies and procedures (ISO 2016:8; Bantin 2008:233; Okello-Obura 2011:6). These should reflect an application of the regulatory environment to the organisation’s business processes (Hamidovic 2009:1). The regulatory environment is normally made up of the following:

- Statutes, case law and regulations such as those affecting archives, records, access, privacy, evidence, data protection and information.
- Mandatory standards of practice
- Voluntary codes of best practice
- Voluntary codes of conduct and ethics
- Identifiable expectations of the community about what constitutes acceptable behaviour for the specific sector or organisation (Hamidovic 2009:1).

This study has shown that apart from procedures, no standards have been adopted to promote the creation of authentic digital records. According to ISO 15489-1 (2016: v), records management entails “taking appropriate action to protect their authenticity, reliability, integrity and usability as their business context and requirements for their management change over time.” Having standards and procedures regulating the creation of authentic digital records is crucial in enabling records to effectively serve as evidence of business transactions. For example, ISO 16175-3 (2010) provides specific general requirements and guidelines for records management and gives guidelines for the appropriate identification and management of evidence (records) of business activities transacted through business systems. Yet, another useful one is ISO 23081-1 (2006), which gives guidance on records management processes metadata for records. Seymour (2017:35) asserts that standardisation is fundamental to ensuring that digital records are controlled. They also enable the capturing and preservation of records, including the evidence of access or change to such records.

5.3.2 Procedures Used by ICT Professionals to Declare Records Authenticity

ICT professionals have a way of ensuring that digital records in an information system retain their integrity and identity and thus their authenticity. Records authenticity is a fundamental concept in archival science and has a theoretical foundation (Rogers 2016:17). For ICT professionals, authenticity of digital records is ensured through the following:

- Segregation of duties
- Inbuilt computer security mechanisms

- Usernames and passwords
- Audit trails
- People outside government cannot access GABS.
- Records in the system cannot be deleted, only cancelled.

For ICT professionals, much reliance is placed on the use of equipment to maintain the authenticity of records. Rogers (2015:94-95) 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 (2015:95), 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. For example, the British Broadcasting Corporation (2010:7) prescribes through its Records Management Standard that it should be possible to provide adequate protection of the integrity of records for auditing purposes.

5.3.3 Procedures Used by Auditors to Authenticate Digital Records

When auditors undertake an audit assignment of financial records produced by business systems, they may ask a number of questions in order to determine whether the audit evidence can be reliable and authentic (Illinois Department of Revenue 1998:1-2). 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. These questions listed are just a snap shot. Answers to these questions facilitate the audit engagement.

The results of the study indicate that auditors (both internal and external) are mindful of the authenticity of records in GABS. Specific results of the study indicated that:

- the system has the capability to create and maintain authentic records, but human interventions can tamper such authenticity if controls are not in place
- auditors mostly use audit software to conduct analytical procedures from whose results they can deem records in the system to be authentic
- the authenticity of digital accounting in GABS has been questioned before
- there are instances where records were rejected in the audit process due to their lack of authenticity. In addition, the auditors have indicated that when records are not authentic, they call for them to be corrected, if not completely, then in such a way that, when proper records are availed, the records are not rejected
- GABS as a business information system has functionalities for ensuring that it creates and maintains authentic reliable digital accounting records
- certain factors are necessary for the acceptance of digital accounting records in the audit process
- the audit process requires authentic reliable records for records to be acceptable in the process. It has to be followed during the process of auditing.

Auditors rely heavily on records to facilitate their auditing assignments because of their significance in the audit process (Ngoepe 2004:8; Ngoepe 2012:2). In a study that used informetrics to analyse the general reports of the AGSA for the years 2005/06 to 2009/10, it was revealed that records management contributed to audit opinions (Ngoepe & Ngulube 2013:59). A similar finding was arrived at by David (2017:13) whose study revealed that inadequate records management practices were associated with adverse and qualified opinions and, in some cases, unqualified opinions in Zimbabwean government entities.

The centrality of records management to the whole audit process is underscored by Duranti (2012) who calls for records management practitioners to help regulatory and auditing bodies as well as policymakers see the need to embed record-keeping requirements in any activity they regulate, audit or control. Answering that noble call by Duranti (2012) was a proposed framework to embed records management in the audit process (Ngoepe & Ngulube 2016:901). The framework recognises the role played by records management in every step of the audit process because records support the audit process by providing required information and documenting the audit process itself.

5.3.3.1 Capability of GABS to create and maintain authentic records

Business information systems are expected to create and maintain trustworthy and thus authentic and reliable digital records (State of Alaska 2009:6). Digital records need to be kept authentic for as long as they are needed for business transactions (Jansen 2014:39). It is for the undisputed reason linking records management with the audit process that auditors demand authentic records when auditing. One finding of the study indicated that GABS as a business system was well placed to create and store authentic accounting records because of system-built database security features. Since records in the digital space are prone to accidental or deliberate alteration (Boudrez 2005:1; Xie 2011:577), maintaining the authenticity of such records once created is of paramount importance (Duranti & Blanchette 2004; Mason 2007:32). That can be done through authentication of digital records in the system (McDaniel 2006:4; Mason 2007:32). GABS demand authentication of users before they can transact business through the system. Firewalls, passwords and segregation of duties are some of the procedures in place to ensure that only authorised personnel get access to the system to transact business. As outlined by Gibson (2001:65-66), Duranti (2001:44-48), InterPARES (2005) and Duranti (2010:83), the following can be used to assert records authenticity in an information system:

- Defined records access privileges.
- Established procedures to prevent loss or corruption of records through intentional or inadvertent unauthorised additions, deletions or alterations.
- Maintained audit trails of transmissions and of access to the record system.
- Established methods and rules for authentication.
- Designed profile, including fields that allow the verification of records identity and integrity.

- Established procedures to prevent the loss of records due to factors such as technological obsolescence (of hardware, system software, and storage media such as: storage devices, access methods, and database management system).

5.3.3.2 The use of audit software in the audit process

The use of ICTs to conduct businesses has resulted in digital records being created and stored in business systems, including the ones used for accounting (Elefterie & Badea 2016:1). This therefore entails that auditors should be able to audit financial statements in the digital environment. They should be able to select, gather, analyse and report, and thus help in adding credibility to audit findings, conclusions and recommendations (Carroll 2006:63). The use of audit software has therefore become a necessity in the audit process where digital information systems are used to perform accounting duties. This makes IT a critical tool in the financial audit process in the increasing use of complex computerised accounting systems and the high volume of transactions recorded accounting (Elefterie & Badea 2016:1). As a result, organisations started using audit software that have come to be known as CAATs (Computer Assisted Audit Techniques).

Prior to commencing the audit process using CAATs, auditors check for basic internal control functions contained within a business system. Some of the items they look for include, but are not limited to, the following:

- System threat and risk analysis
- Limited access to the digital system
- Access authorisation or security codes
- Unalterable date-stamping of transactions and transaction files
- System and data access logs
- Data alteration logs and preservation of original unaltered data record
- Rejected transaction or transmission procedures and logs

- Regular review of access alteration and rejection logs or trails (Illinois Department of Revenue 1998:2).

The auditors (both external and internal) who took part in this study indicated that one of the procedures they relied on to audit records in GABS was the use of auditing software. They both indicated that the use of audit software such as CAATs and ACL was one way of checking records authenticity in the system.

The computerisation of accounting functions has meant that auditing has to use ICTs like CAATs in the audit process. Examples of CAATs include Audit Generalised Audit Software (GAS). The benefits of computerised auditing are undeniable (Kanellou & Spathis 2009:174; ACCA 2011:4; Moorthy et al. 2011:3523; Rezaei 2013:90). Auditors use GAS 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, Lee, Neo & Shuling 2005: i). GAS can browse, analyse, sort, summarise, stratify, sample and apply calculations, conversions and other operations to audit a full set of accounting data (Ahmi & Kent 2013:89).

It is clear from the study findings that with GAS such as ACL and IDEA, auditors can check the authenticity of records in GABS. Some of those checks include running analytical tests such as data verification, data formatting, checking for data completeness, data verification, checking for gaps and totals controls.

5.3.3.3 Rejection of questionable digital records in the audit process

One notable finding of this study was that there were instances in the past when the authenticity of records in GABS was questioned. This led to records availed for auditing to be rejected because they were not trusted to be tendered as evidence in the audit process. In the South African public sector, Mulaudzi et al. (2015:2) note that auditors have rejected digital records as evidence during audits because their authenticity was questionable. According to Park (2001:272), "when a record is what it purports to be, the record is genuine." This presupposes that if a record does not purport what it claims to be, it cannot be genuine. Digital records are problematic to manage because they can easily be tampered with or corrupted either by accident or through deliberate means (Duranti 2009:52). This technological issue thus negatively affects auditing in a digital environment. It makes it difficult to determine the authenticity of audit evidence (records) (Park 2001:288; Barrister 2006:19). What compounds this problem is that a criterion used by auditors to judge the authenticity of digital records in order for them to support the audit process is not clear (AGSA 2014:68).

5.3.3.4 Requisite factors for acceptance of digital accounting records in the audit process

This study has unearthed factors that are necessary for the acceptance of digital accounting records to be acceptable in the audit process. These factors are the following:

- Accuracy and completeness of records.
- The data should be from the production environment of the GABS database.
- If the data are extracted from the system, the extraction has to take place in the presence of auditors.
- The said extraction has to be witnessed by auditors if it is not them who do the extraction.
- A checklist of reports indicating that computer system controls are working.
- Policies governing information security.

5.4 Skills and Competencies for Authenticating Digital Records

The third objective of the study was to establish skills and competencies needed by auditors, ICT specialists and Records Managers to authenticate/establish the authenticity and reliability of digital records created and stored in GABS. The skills and competencies pertained to Records Management Professionals, ICT specialists and auditors.

5.4.1 Skills and Competencies Needed by Records Managers

The advent of e-government has meant that governments produce digital records in the delivery of public services (Kamatula, Saurombe & Mosweu 2013:124; Muchaonyerwa & Khayundi 2014:42). According to Wamukoya and Mutula (2005a:73), managing records in a digital environment poses some challenges to staff members in organisations as new technologies require new skills and competencies to cause them to operate in such an environment. It was this recognition that this study asked records management professionals to state skills and competencies they needed to authenticate digital accounting records in GABS. The following were listed as such skills and competencies:

- Knowledge of digital preservation and computing skills
- Electronic records management
- Enterprise Content Management
- Legal aspect of information
- Analytical and planning skills
- Metadata and auditing
- Effective communication and consensus building skills
- Appreciation of secure digital signatures platforms
- Security and privacy control

The digital age poses a challenge in the skills set of archives and records management professionals as they need to cope with the changes and complexities associated with the records management digital environment. According to Eastwood (2006), archivists need to have a variety of skills, which comprise designing, implementing and managing record-keeping systems, especially in the digital environment. They need to be able to analyse business functions, activities, procedures and needs (Eastwood 2006:166). Eastwood refer to these as “archival analysis.” Equally important are metadata schema and the analysis of the impact of technology on records management.

The National Archives of Australia (NAA) (2015) recognises the need for records management professionals to possess requisite competencies and skills to manage records in the digital age. It was imperative for the NAA to ensure digital continuity, so it came up with the development of a digital information and records management capability matrix for records managers (National Archives of Australia 2015:3-10). Faced with the need for digital continuity, the NAA (NAA 2015) came up with the following as skills needed by archives and records management professionals in the digital age:

- Awareness of legislation, standards and policies affecting information management
- Information governance and business risk mitigation
- Metadata
- Risks to information
- Retention and destruction of information
- Access to information
- Standards and best practices
- Specialist technologies
- Communication and leadership
- User experience

In the context of Botswana, available empirical studies have shown that archives and records management professionals lack skills and competencies to manage digital records (Tshotlo 2009:73; Keakopa 2010:67; Moatlhodi & Kalusopa 2016:13; Mosweu 2014). For example, in a study that assessed digital records readiness at Botswana’s Ministry of Labour and Home Affairs, 80% of the records personnel had not been trained on digital records management, while 52% felt their capacity to manage records was low. This was despite the fact that the study took place at the time when the ministry was about to implement the Botswana National Archives and Records-led project dubbed the National Archives and Records Management System (NARMS). The project was actually the implementation of a government-wide digital records management system. Elsewhere, at the Ministry of Trade and Industry where an

EDRMS was implemented but poorly adopted and used, it emerged that it was due to poor capacity of records management staff (Mosweu 2014:105).

Poor capacity to manage digital records is not peculiar to Botswana. This has also been reported in other ESARBICA countries (Wato 2006:74; Kemoni 2009:194; Kamatula 2010), African countries (Mnjama & Wamukoya 2007:279; Asogwa 2012:202; Abuzawayda, Mohd & Mohd 2013:250; Adu & Ngulube 2017:1131) and the globe as a whole (also in China, Iceland and Malaysia just to name a few) (Saman & Haider 2012:8; Wang 2009:7).

5.4.2 Skills and Competencies Needed by ICT Specialists

The ICT specialists indicated that in order to establish the authenticity of digital accounting records created and stored in GABS, the following skills and competencies are a basic requirement:

- System design
- Business process analysis
- Business rules
- Data analytics
- Computer forensics and security
- Database administration

ICT specialists play a central role in the implementation of information systems. They build and maintain the ICT infrastructure through which the application software runs. They provide technical specifications needed to run a specific software (Waldo 2006: 2). This is done through working with accountants who provide the functional specifications commonly referred to as system user requirements. ICT experts also maintain the database for the system. ICT professionals are also responsible for the protection of the network, infrastructure and other areas of information technology. A secure network is essential for an operational information system. The following are the responsibilities of an information technology security professional:

- Developing and designing security devices and software to ensure the safety of clients' or internal products and information
- Managing security measures for information technology system within a networked system
- Operating regular inspections of systems and network processes for security updates
- Conducting audit process for initiating security and safety measures and strategies
- Customising access to information per rules and necessity
- Maintaining standard information security policy, procedure, and services (Easttom 2018).

In recognition of the skills and competencies required for digital continuity, the National Archives of Australia issued the generic capabilities required by ICT experts to run and maintain the Digital Continuity programme (National Archives of Australia 2015). The specific capabilities are listed in Table 2.1.

5.4.3 Skills and Competencies Needed by Auditors

Auditing in a digital environment requires appropriate skills and competencies among auditors. This is particularly apparent in the digital environment where ITCs are increasingly deployed to improve audit efficiency and effectiveness (Trompeter & Wright 2010:671). Various bodies such as the Association to Advance Collegiate Schools of Business, Institute of Management Accountants and the American Accounting Association all stress that accountants need to be equipped with specific tools, knowledge, skills and techniques of information technology to enable to conduct audit assignment assignments in the digital environment (Tudor, Gheorghe, Oancea & Şova 2013:674). Auditors are trained as accountants before they do audit work (IFAC 2005:9).

This study has revealed that auditors need to be equipped with the following skills and competencies for them to audit financial statements in a digital environment:

- Data analytics

- Business rules and business process analysis
- Knowledge of and the use of CAATs
- An understanding of system design and development
- Information system audit expertise
- Monitoring and evaluation
- Presentation and creative skills

In totality, the cited skills and competencies would enable auditors to do their work with little inhibition. Without adequate training and insufficient knowledge in the use of ICTs, auditors may not spot such accounting information systems, risks inherent in the audit process (Austen, Eilifsen & Messier 2003:4). Authors such as Curtis, Jenkins, Bedard and Deis (2009:83) note that, generally, the use of information systems such as ERPs has changed the nature of business with automated controls meant to produce more reliable financial statement information. The auditors added that without extensive systems knowledge, auditors may face the difficulty of understanding the complex supporting the business processes of their clients. It is therefore of paramount importance that auditors are capacitated to deal with audit issues in the digital space. For example, Curtis et al. (2009:81) cautions that although automated controls may contribute to efficiency, too much reliance on them with inadequate systems knowledge could be problematic if technology savvy employees circumvent them.

In terms of using CAATs in the audit process, Sayana (2003:1) says that three instances are applicable for using computerised audit software. The first one is that the auditor needs to have access to a client's "live" data for purposes of downloading. Thereafter, the data have to be transferred to the auditor's computer for analysis and either the auditor or the ICT audit expert in the audited organisation can do this. Secondly, the auditor must be knowledgeable about the support system and the data (Sayana 2003:2). The last instance is that the auditor must possess the skills to be able to discern the type of analysis to be performed and this Sayana (2003:2) refers to as the knowledge of the data to be verified and tested, and of the business environment. Some of these requirements border on data analytics, which was cited as one of the skills and competencies required by auditors in the digital environment.

5.5 The Management of Authentic Digital Records to Support Audit Processes

Regardless of their format, records need proper management across their whole life cycle. The purpose of this objective was to investigate digital accounting records practices from their creation through to their disposal, including their preservation over time.

5.5.1 Records Capture in GABS

When organisations perform their mandate, they create records as evidence of the performance of the mandate. Those responsible therefor can use such records to ensure accountability, including enabling organisations to meet legal, regulatory and financial requirements, and to protect their assets and rights (Ndenje-Sichalwe, Ngulube & Stilwell 2011:265). This study revealed that various records are created through the system, either by direct capturing or by being imported from other government information systems. These records emanate from different accounting and budgetary processes such as payables, receivables, budgeting and after spending. This function of GABS affirms it as a fit-for-purpose business information system that is well placed to capture records of the accounting and budgetary process as mandated to the AGD by the Government of Botswana.

ISO 15489-1 (2016) provides the criteria for the organisation to create and maintain authentic, reliable and usable records. These criteria, among others, are to: determine the kind of records created in each business process and information needs to be included in the records; decide what form and structure records should be created and captured and the technologies to be used; determine the metadata to create with records and through records processes and how the metadata will be linked and managed; and decide on the organisation of records so as to support requirements for use.

Records can be used to ensure accountability to make people and businesses account for their actions and obligations, and to indicate when there is a need to prove that organisations have complied with legal or regulatory requirements or recognised best practice. Records enable organisations to meet legal, regulatory and financial requirements, and to protect their assets and rights.

5.5.2 Records Retention and Disposal in Gabs

Records serve a purpose in an organisation, after which they can be disposed of. This means that records are not supposed to be kept beyond their usefulness to the creating agency. The National Archives of UK (2012:41) cautions that in order for organisations to evade retaining records for longer than required for business purposes, organisations need to have records disposal policies. A records disposal policy can be subsumed in an overall organisational records management policy or it can be a separate document. The policy usually provides an overview of and serves as an introduction to a more detailed document, the disposal schedule or, for large organisations, disposal schedules (National Archives of UK 2011:6).

This study discovered that BNARS has issued a records retention and disposal schedule for common records across government ministries and departments, including financial records. Other than that, the AGD issued some Financial Instructions and Procedures which contain some records retention periods. It is, however, notable that GABS as a business system does not have a records retention and disposal schedule configured into it as it would have had it been a record-keeping system. The absence of well-defined records retention and disposal schedule suggests that when GABS was designed, records management professionals were not involved from the onset, even when the system was upgraded. Secondly, this suggests that BNARS was also not involved at the design stage, although, legally, it is the agency responsible for public sector records management. Ndenje-Sichalwe et al. (2011:272) assert that systems managing records should be able to facilitate and implement decisions on records retention and disposal.

Since GABS was implemented, digital accounting records have resided in the system. It would seem this is not a good option for preservation as the system has become overloaded with old data or records and this often makes the system slow. Although government departments and ministries in Botswana have computerised some of their operations, they have done so without a framework for managing their digital records. In view of the absence of e-records management policy and programmes within government, there is an eminent danger that records generated may not be retained and preserved as digital archives (Moloi 2009:110-11). To bring this point home, the ICA/IRMT (2016:5) avers that the maintenance of the integrity of digital records is a massive challenge because key stakeholders such as Senior Managers, Programme Planners, IT Staff, Legal Specialists and Development Planners, are often not aware of the risks posed by technology. They often assume technology would solve problems, while, in fact, it exacerbates them.

5.5.3 Disaster Management for Records

The safety and preservation of records is always threatened by the possibility of a disaster (Government of South Australia 2007:6). The following include some of the possible disasters that can affect records:

- Natural events or hazards, including bushfires, floods, vermin, lightning strikes, windstorms
- Structural or building failure such as malfunctioning sprinklers, heating or air-conditioning systems, leaks in roofs, poor wiring, sewer/ storm water/ drainage failure, energy failure
- Industrial accidents such as nuclear or chemical spills, fire, explosions, gas leaks, falling object damage
- Technological disasters such as viruses and computer equipment failures
- Criminal behaviour such as theft, arson, espionage, vandalism, bombing, demonstrations and terrorism
- Accidental loss through human error (Latham 2012:1)

Pertaining to disaster management for accounting records created and stored in GABS, this study discovered that the DIT has an Institutional Disaster Plan for the accounting records. Disaster management for records management at the DIT is part of the overall institutional disaster management for data in the various business information systems implemented in the government. According to the Government of South Australia (2007:9), "a counter disaster management for records should take place in the framework a government agency's business continuity plan." Although the DIT has done well to have an institutionalised disaster management plan to safeguard records created and stored in GABS, a worrisome factor is that accounting records are stored within the DIT's two main data centres in Gaborone, meaning within the offices of the data. This is bad practice as the department can still lose its vital data should a disaster strike the two data centres. According to the Australian Capital Territory (2008:7), remote storage is ideal for vital records as part of business continuity planning.

5.5.4 Integration of GABS with other Information Systems

GABS have been integrated with quite several other government information systems as part of the overall e-government drive. The integration has been deliberate owing to its promotion of efficiency in the delivery of services. Business information systems lack the functionalities of records management systems and therefore do not have the longevity to manage digital records over time (State Records Office of Western Australia 2015:9). Like most business information systems, transactional records created through GABS are not managed through a record-keeping system. The IRMT (n.d) also notes that often, ICT systems are introduced without regard for processes and controls necessary for the capturing, long-term safeguarding and accessibility of digital records. In such instances, design specifications for business systems would include record-keeping functionalities or integration with a record-keeping system to ensure that they are managed accordingly (State Records Office of Western Australia 2015:9).

This study revealed that GABS, as a business information system is not integrated with any record-keeping system although it has that capability. It can be integrated with the CRMS of the Department of Administration of Justice, implemented to manage court records (Mosweu 2012:71) but that was not done. It can also be integrated with the Document Workflow Management System (DWMS) deployed at the Ministry of Investment Trade and Industry (MITI) (Mosweu 2014). Rather, it is integrated with other business information systems. For purposes of managing digital records, this does not guarantee their availability and accessibility over time, but only for the Government of Botswana's e-government drive. For the e-government agenda, it is a step forward as the seamless flow of information between the systems at least facilitates the management of financial records. This is because the Government of Botswana views the use of ICTs in service delivery as the driver of the country's developmental agenda hinged on economic growth, poverty reduction and global competitiveness (Nkwe 2012:14).

5.6 Recommendations Offered by Study Participants

This section briefly discusses various recommendations offered by the study participants, being records management personnel, ICT professionals and auditors.

5.6.1 Recommendations by Records Management Personnel

Records management professionals made the following recommendations pertaining to the study:

- Capacity building for records management on the management of digital records.
- Involvement of records managers in the design and implementation of business systems.
- Development of guidelines for the management of authentic digital records.
- Collaboration by records, legal and ICT experts to find solutions for the management of digital records.
- Amend and strengthen the legislative framework.
- Development and implementation of a digital records strategy.
- Use of digital signatures to authenticate digital records.

5.6.1.1 Capacitating records management staff to manage digital records

A successful records management system is only possible if the people who create and use records to serve their business mission support it (Kenosi & Mosweu 2018:222). In this context, these people refer to personnel who create, use and manage records. Staff training in the field of archives and records management is an important part of the records management programme. Literature on the management of records in the ESARBICA region is abound with staff that are ill prepared to manage digital records (Mnjama & Wamukoya 2007:279; Kemoni 2009:194; Luyombya 2010:60). In recognition of the need for capacitated records management in the management of digital records, the National Archives of Australia developed a digital information and records management capability matrix for records managers to enable them to cope with the requirements for the management of digital records (National Archives of Australia 2015:3-10). Records management professionals therefore need skills and competencies to effectively manage digital records, and these include, but are not limited to, knowledge of digital preservation and computing skills, enterprise content management, legal aspect of information, analytical and planning skills, analytical and planning skills, analytical and planning skills, metadata and auditing, effective communication and consensus building skills, appreciation of secure digital signatures platforms and security and privacy control**.**

5.6.1.2 Involvement of records managers in the design and implementation of business systems

Systems that produce digital records fall into two categories. The first category includes electronic records and document management systems (EDRMS) software and Enterprise Content Management (ECM) systems with records management functionalities (Kastenhofer 2016:3). The second category is that of the more common transactional or business systems that transact organisational business and produce records although they may lack records management functionalities (United Nations 2006:5; Cumming & Findlay 2010:269). According to McLeod (2012:191), business systems are not designed to manage records in the long term or even the medium term. Unless the business process requires that records produced by business systems must be captured as records in record-keeping systems, they will just remain undeclared in their home environment (Johnston & Bowen 2005:132). This scenario applies to GABS. Since it is not a designated record-keeping system, records that were produced by the system since its implementation in the system still reside in the system and actually clog it so much that the system is overloaded and has become slow. To circumvent this challenge, records management professionals need to be involved in the systems development lifecycle and capital and investment control processes to ensure that permanent digital records are identified and scheduled accordingly (NARA 2018:6). Alternatively, business systems can be integrated with existing EDRMS to enable records created by business systems to retain their ability to serve as evidence of performed transactions because they retain their authenticity. In order to come to that, the IRMT (2009:2) advises that a digital readiness assessment can first be carried out to determine whether records management requirements have been integrated in ICT systems in order to inform what needs to be done.

5.6.1.3 Development of guidelines for the management of authentic digital records

Records management personnel have recommended that BNARS develop guidelines to be used by government ministries and departments. Since there are currently no such guidelines in place, it can benchmark with other archival organisations in other countries. The South African National Archives and Records Service has developed and implemented a digital records strategy in the form of a policy document known as *Managing electronic records in governmental bodies: policy, principles and requirements* (National Archives and Records Services of South Africa 2006:4). The strategy provides guidance to governmental bodies and enables them to comply with legislative requirements regarding the management of digital records.

BNARS can also learn from other developed countries such as Australia with their Public Record Office Victoria, which has developed a standard for the management of digital records. This standard is known as ‘Management of Electronic Records (PROS 99/007)’, also known as the VERS Standard (Public Record Office Victoria 2003:3). The goal of the Victorian

Electronic Record Strategy (VERS) is the cost-effective long-term preservation of digital records. The NARA (2018) has also issued a digital records management directive that by 31 December 2019, all permanent digital records in federal agencies should be managed digitally to the fullest extent possible for eventual transfer and accessioning by NARA in digital form (NARA 2018:2). Nkala et al. (2012:112) argue that in the context of a digital environment, archival institutions should thus strive to facilitate the establishment of policies, procedures, systems, standards and practices that can be used by records creators to create and maintain authentic, reliable records that can be preserved over time. The guidelines can cover a number of areas such as the following:

- Procedures for scheduling, managing and transferring permanent digital records to the national archives.
- Policies for the use of digital signatures that support the creation and management of permanent digital records.
- Notification and reporting procedures for unauthorised access, use, alteration, alienation or deletion of digital records.
- Incorporation of records management requirements into Systems Development Lifecycle and Capital Planning and Investment Control processes.
- Integration of records management into IT system design and development.
- Insertion of clauses in contracts to safeguard government-owned permanent digital records, information and associated data that are created, maintained and stored on cloud or social media platforms owned by third-party vendors (NARA 2018:8).

Moatlhodi and Kalusopa (2016:11) discovered a lack of guidance on the part of BNARS when the then Ministry of Labour and Home Affairs implemented the National Archives and Records System's (NARMS) EDRMS project. An earlier study by Ramokate and Moatlhodi (2010) revealed that due to a high staff turnover of archives and records management professionals, BNARS lacks capacity to provide guidance for records management services in the public sector.

5.6.1.4 Collaboration by records, legal and ICT experts

Several studies in Botswana specifically (Moloi & Mutula 2007:298-9; Mosweu 2014:105; Moatlhodi & Kalusopa 2016:13; InterPARES 2016:18) and the ESARBICA member countries (Wamukoya & Mutula 2005b:75; Nkala et al. 2012:114; Muchaonyerwa & Khayundi 2014:45; Malanga & Kamanga 2018:8) have shown that records management personnel lack the capacity to manage digital records. Therefore, alone, they cannot hope to deal with issues pertaining to the management of digital records, including the maintenance of their authenticity. It is therefore crucial that they collaborate with IT experts to address some issues related to the management of digital records. For example, ICA (2005:57) says that:

> Little is different with electronic records. Institutions may find that the necessary skills are spread through a greater number of people. For instance, the record-creating organisation is still required to have the basic skills to ensure that retention and disposal schedules are developed and applied to digital records. But to apply the schedules effectively, and to audit that they have been applied, may require the advice or cooperation of someone with an understanding of the software and hardware systems in which the records exist. Such understanding can typically be found in people described as systems analysts.

Collaboration with ICT specialists such as Chief Information Officers, Chief Data Officers, Chief Technology Officers and IT Enterprise Architecture Staff to identify data maps for systems containing permanent digital records is thus unavoidable (NARA 2018:6). While it is appropriate that records management professionals collaborate with ICT specialists to address issues of digital records management, it is also crucial to note that the same ICT specialists are unlikely to have the records management skills necessary to develop the schedules in the first place. Keakopa (2002:47) calls for synergy to be created between Archivists, Records Managers, Legal staff, Programme Managers, clients and counterparts in IT for the development of record-keeping systems. ICT experts are knowledgeable when it comes to systems design, while records management professionals are records gurus. Legal experts can give insights into legal implications related to creating systems that manage authentic digital records.

5.6.1.5 Amend and strengthen the legislative framework

The management of records should be done in a government environment governed by appropriate legislation, which provides guidance, inclusive of digital records (Bantin 2008:233; Luyombya 2010:51). Archival legislation in Botswana is weak regarding its guidance on the management of digital records (InterPARES 2016:10). This is even though the National Archives and Records Services Act was amended in 2007 to cover digital records management (Ngoepe & Keakopa 2011:155; InterPARES 2016:10). Compared to other archival legislation in other countries such as in South Africa and Canada (Government of South Africa 1996; Government of Canada 2004, amended in 2016) just to cite two examples, Botswana is lagging behind. Amending archival legislation in Botswana to enable it to provide guidance on the management of digital records is therefore overdue and needs to be done urgently. Okello-Obura (2011:3) observes that ineffective and outdated laws can affect how records are managed. He adds that many developing countries have weak laws or inactive legislative provisions, and this hinders good archives and records management. The ICA (1997:19) also observes that legislation governing many aspects of information creation, management, use and preservation has not kept pace with the rapid change in technology, archival legislation included.

5.6.1.6 Development and implementation of a digital records strategy

One other recommendation offered by records management personnel was that BNARS should develop a digital records strategy to guide the management of digital records in the public sector. There is an opportunity by BNARS to develop such a strategy and utilise the expertise of a fellow ESARBICA member country such as South Africa, which has a strategy in place. Among other principles of records management, the strategy should endeavour to promote the management and preservation of authentic digital records (National Archives and Records

Services of South Africa 2006:24). The digital records strategy should conform to international best practices in records management in all respects. ISO 23801-1 (ISO 2006:1) is a metadata standard for records management processes. Among what the standard lays down is the need for digital records management systems to have record-keeping metadata which helps to ensure that the authenticity of records is maintained after creation (ISO 2006:1). In their recognition of digital records as part of heritage, the UK National Archives' Digital Records Strategy encourages the development of extraordinary capabilities to ensure that digital records can be kept because "we use them to help understand the past, make sense of the present, and to guide us for the future" (UK National Archives 2017:2).

BNARS can also adopt and adapt the National Archives of Australia Digital Continuity 2020, a digital records strategy that plays a key role in supporting the Australian government's digital transformation initiatives and drives e-government (National Archives of Australia 2015:3). Three principles underpin the strategy and the following two resonate with Botswana as a country grappling with e-government:

- Information is valued: Information is regarded as a strategic resource just like human resources, finances and equipment. Digital information can facilitate efficient service delivery, improve business decisions, and create new opportunities for process and service redesign, and innovation.
- Information, systems and processes are interoperable: Prior planning should be undertaken to ensure that public agencies implement interoperable systems. The design and integration of these systems should be planned from the start.

These principles can benefit BNARS in its development of a digital records strategy. The Danish National Archives requires public sector bodies to notify it of new ICT systems to be implemented so that they are assessed for their abilities to produce and store records worthy of permanent preservation. If the latter is the case, the Danish National Archives has to make sure that such records can be exported to the Danish National Archives' submission format (Danish National Archives 2013:4). By developing a digital records strategy to guide the transformation to managing records in the realm of e-government, BNARS would be actually performing its legal obligation of advising government ministries and departments about the care, preservation, custody and control of public archives as prescribed by the National Archives and Records Services Act, Part III Section 5(4)(e) (Government of Botswana 1978).

5.6.1.7 Use of digital signatures to authenticate digital records

Digital signatures can be used to authenticate digital records in a similar way that a hand-written signature can be used to authenticate the originator of a digital document. It is a piece of data that cannot be forged that asserts that a certain person either wrote or otherwise agreed to the digital document to which the digital signature is attached (Centre for Technology in Government 2003:2). Minnesota State Archives (2012:4) defines a digital signature as:

> A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.

The Center for Drug Evaluation and Research (2017:2) avers that a digital signature as a method of originator authentication confirms the identity of the signer and enables the integrity of data to be verified. The Minnesota State Archives (2012:4) indicates that digital signatures are advantageous in that they provide a unique identifier and link the signature to the record. The use of digital signatures to authenticate records in GABS is actually a legal requirement under the Electronic Communications and Transactions Act (Government of Botswana 2014). It is a prescription under the Act that the digital signature may not be denied legal effect, validity, or enforceability solely because they are in digital form. In the context of this study, it is clear that proper records management plays a significant role in the audit process (Ngoepe & Ngulube 2015:2). It has become even clearer that in the networked office environment determining their authenticity is difficult (Katuu 2016:123), hence this study’s endeavour to propose a framework to guide auditors in assessing the authenticity of digital records to support the audit process.

5.6.2 Recommendations by Auditors

Both internal auditors at the Department of Internal Audit and external auditors at the Office of the Auditor General of Botswana made some recommendations towards maintaining records in GABS authentic after creation. These are:

- Capacity building for auditors to enable them to audit in the digital environment
- Segregation of duties with the system
- Involvement of auditors during systems design
- Minimum human interference in the processing of records

5.6.2.1 Capacity building for auditors

The computerisation of business processes, including the function of accounting and financial management, has ushered in an era where computers and networks provide most of the information required for auditing (Oginga 2013:1). Modern day auditors have to use computers as audit tools, audit automated systems and data, understand the business purposes for the systems and understand the system operating environment if they are to be effective. This study has revealed that some of the auditors in this study lack the capacity to effectively audit in the digital environment because they were trained as financial auditors, not information systems auditors. Therefore, they advocate for capacity building to enable them to use CAATs in auditing. They particularly desired to be trained and certified in Oracle, COBIT and ACL. That would expose them to data analytics, which is crucial in the auditing assignment (McCafferty 2017). If they lack capacity to use them, they would not be able to determine whether application controls are working as they should, as they are built into the system. The effective use of CAATs enables an objective and independent assessment of accounting records (Institute of Chartered Accountants in England and Wales 2009:6).

5.6.2.2 Segregation of duties within the system

Ernest and Young (2010:1) introduced a risk management initiative whereby no individual should have excessive system access that enables them to execute transactions across an entire business process, as that that can have an impact on financial statements. It provides some form of checks and balances. Little and Best (2003:419) argue that the segregation of duties as a critical component of internal control is meant to reduce opportunities for fraud by individuals for purposes of personal gain. Coleman (2008) observes that segregation of duties is meant to prevent conflict of interest, the appearance of conflict of interest, wrongful acts, fraud, abuse and errors. It is also meant to detect control failures that include security breaches, information theft and circumvention of security controls. The purpose of security controls is meant to protect information systems against attacks on the confidentiality, integrity and availability of computer systems, networks and the data used. The recommendation to segregate duties is not surprising as one auditor participant had remarked, "employee from one ministry was able to make fake payments using GABS." That would have been avoided had proper controls been exercised.

5.6.2.3 Involvement of auditors during systems design

The auditors in this study recommended that auditors should participate in system design from the onset as that would make their task easier in the future. Notably, this recommendation by auditors themselves clash with IT Standards, Guidelines, and Tools and Techniques for Audit, Assurance, and Control Professionals (ISACA 2010:10). It requires that auditors be independent auditee in both attitude and appearance. However, the assertion by the study auditors is supported by literature. Maher and Akers (2003:13) undertook a study on internal auditor participation in systems development projects and one of the responses by Chief Executive Auditors revealed that Chief Audit Executives believed that internal auditors should have some type of involvement throughout systems development projects for purposes of providing information on controls. Chief Audit Executives do not perceive auditor independence as critical for system development audits and would rather have auditors as consultants. This is consistent with the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing, which supports internal auditors as consultants, but cautions them to maintain their objectivity and not assume management responsibilities (Institute of Internal Auditors 2016:2). Other than that, the G3 Use of CAATS supports the embedding of audit software during system design and allows the information systems auditor to take part and develop techniques for maintaining the organisation's application programmes or systems (ISACA 2008:4).

5.6.3 Recommendations by ICT Professionals

ICT professionals in this study made three recommendations. These recommendations are presented in the next sections. The first one was to migrate old records in the system to a data warehouse for preservation. The second one was to use a data centre outside the City of Gaborone as a disaster management measure to ensure continued availability of records. The last one was to implement solutions to monitor database and system administrators as a way to protect the authenticity of records in GABS.

5.6.3.1 Migration of records in the system to a data warehouse

The first one related to the need to migrate old records in GABS and move them to a data warehouse. The issue at hand is that GABS is not a record-keeping system and does not have a records retention schedule configured into it. Still, records in the system have to be disposed of. Disposal of records in this context means the removal of records from the business system which may involve their destruction or transfer to another entity, which can be an archive or data centre (ICA 2013b:14). Since GABS was implemented in 2004, records have resided in the system. That has actually impaired system performance.

As a business system, it lacks all the functionalities of a record-keeping system, which ensures that the evidence (records) of business transactions is captured and kept authentic (ICA 2008:8). Migration of records from old systems to newer ones or transferring them to an archive is a common feature in information systems (ICA 2013b:13). However, care and caution should be taken when migrating digital records, as their authenticity is threatened when they are transmitted across space or time (Bearman 2007:24).

5.6.3.2 Building of a data centre outside the city of Gaborone

The second recommendation was that for purposes of disaster management, a data house should be built in a different location outside Gaborone. This is because, currently, DIT data centres are in the two buildings that house its servers, including backup. Disaster management for records should include risk assessment, planning and vital records protection (State of New South Wales 2002:6). Building a data centre away from the current ones (within two buildings housing the DIT) would be a good strategy for the prevention, preparedness for and response to disasters, and the recovery of operations (Government of South Australia 2007:9).

5.6.3.3 Implementation of solutions to monitor Database and System Administrators

The third recommendation was to implement technology solutions to monitor activities of database and system administrators. The role of Data Administrators is to administer, develop, maintain and implement policies and procedures necessary to ensure the security and integrity of the corporate database. The sub-roles can be classified into security, architecture and warehousing and/or business analysis (Peshkar & Ghosekar 2015:42). Other roles may include implementation of data models, database design, database accessibility, performance issues, capacity issues, data replication and table maintenance. The ICT specialists recommended Database Activity Monitoring (DAM) as it provides powerful, immediate, non-intrusive benefits for security and compliance, and a long-term platform for the comprehensive protection of databases and applications (Mogull nd:6). This was since some administrators performed multiple database roles within GABS and the roles fall within the three main categories of operations: database administration, development database administration and data administration.

Roratto and Dias (2014:718) observe that experienced system attackers usually target audit trail/logs and delete them in order not to be detected and to hide the method of attack so as to render system flaws undetectable. By using DAM, threats to the authenticity of records in GABS can be monitored. This is because even administrators can corrupt records accidentally and even intentionally. Thus, the functionalities of DAM provide a secure and permanent storage of log records and enable security breaches to be detected

5.7 Summary

This chapter interpreted and discussed the findings of this study as presented in Chapter 4. It has been noted that legislation exists that guide and impact on digital records management, especially as it pertains to ensuring the authenticity of digital records in the public sector of Botswana. The principal law, which is the National Archives and Records Services Act, lacks the punch needed to guide digital records management practices. However, this Act includes a digital record in its definition of a record. There are others such as the Electronic Records (Evidence) Act, the Electronic Transactions Act and the Cybercrime and Computer Related Crimes Act which prescribe for the protection of the authenticity of digital records in computer-based information systems. The first two recognise the use of digital records in legal proceedings before the courts.

Contrary to expectations, procedures to authenticate digital records have not been developed and implemented by BNARS, although BNARS is aware that public sector bodies have implemented business information systems that create digital records during business transactions. This is despite the department being mandated by the National Archives and Records Services Act to coordinate public sector records management. Meanwhile, ICT professionals use both computer-based information systems general controls and application-based controls to authenticate digital records in GABS. This is opposed to auditors who use CAATs to analyse data in GABS so as to verify its authenticity and acceptability in the audit process. If the data are not authentic and are thus unreliable, it is rejected in the audit process.

In terms of skills and competencies required by records managers, ICT professionals and auditors, it is clear that they need technical competencies and skills if they are to authenticate digital records. This is because records management professionals lack technical skills necessary to fully understand the digital environment. Even auditors, including accountants, lack such technical skills and competencies needed to carry out data analysis, among others, and use CAATs in the audit process. ICT professionals also need specialised technical skills for them to support GABS and even manage its database. Consequently, continuous training programmes meant to improve the skills set of these professionals are a norm. This is because if these professionals are incapacitated, the proper management of digital records in GABS would be problematic and the auditors would be found wanting and challenged by conducting an audit in a complex and technical environment. Their audits would be questionable, and they would not be in a position to authenticate digital records in the system.

The next chapter provides the conclusions, summary and recommendations of procedures used by records management practitioners, auditors and ICT professionals in ensuring the maintenance of the authenticity of records in GABS once created, for purposes of their acceptance in the audit process in the public sector of Botswana. It also proposes a framework to authenticate records in government accounting systems in Botswana to support the audit process.

CHAPTER SIX

SUMMARY OF STUDY FINDINGS, CONCLUSIONS AND RECOMENDATIONS

6.1 Introduction

The previous chapter discussed the findings of the study. This chapter presents the summary of study findings, conclusions and recommendations. Mathipa et al. (2014:191) advise that the last chapter in a thesis should be about the conclusions and recommendations emanating from the study findings. Doing so satisfies the researcher's need to reflect on the journey traversed during the writing of the thesis and to show how the research plan and problem were addressed (Zimu-Biyela 2016:171). The summary of findings, conclusions and recommendations are presented logically and guided by the research objectives of the study.

6.2 Summary from the findings of the Study

This section of the study provides a summary of the study findings with a focus on significant points rather than specific findings (Babbie 2004:490). The study collected data related to the legislative framework for the creation of authentic reliable digital records, procedures for the maintenance of authentic digital accounting records created and stored in GABS, establishment of skills and competencies needed by auditors, ICT specialists and Records Managers to authenticate digital records and the actual management and preservation of authentic digital accounting records for as long as needed for business. Procedures for the authentication of digital accounting records in GABS were established. The main purpose of this study was to develop a framework to authenticate records in government accounting systems in Botswana to support the audit process. Specifically, it endeavoured to:

a. analyse the legislative framework for the creation of authentic reliable digital records stored in GABS in support of audit processes in the public sector of Botswana
b. find procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

c. establish skills and competencies needed by auditors, ICT specialists and Records Managers to establish the authenticity and reliability of digital records created and stored in GABS

d. determine how digital records created and stored through GABS are managed and preserved as authentic and reliable to support audit processes in the public sector of Botswana

e. propose a framework for ensuring that authentic reliable records are created and stored in GABS to support audit processes in the public sector of Botswana.

This chapter suggests a framework to authenticate records in government accounting systems in Botswana to support the audit process. The researcher hopes that the suggested framework would be adopted in the public-sector regularity audit process in the endeavour to authenticate digital records in government accounting systems and make acceptable in the audit process.

6.2.1 Legislative Framework for Managing Authentic Digital Records

The first objective of the study was to analyse the legislative framework for the creation of authentic reliable digital records stored in GABS in support of audit processes in the public sector of Botswana. The following are a summary of the findings:

- An analysis of the legislative framework shows that the National Archives and Records Services Act, the Electronic Records (Evidence) Act, the Electronic Transactions Act, the Cybercrime and Computer Related Crimes Act and the Criminal Procedure and Evidence Act are the main legislation that has a bearing on authenticity of accounting records in GABS.
- The Public Audit Act and the Public Finance Management Act mainly regulate auditing and financial accounting processes in the public sector of Botswana. These two laws are technology neutral and do not prescribe how the authenticity of digital accounting records can be maintained after creation.

- Although the National Archives and Records Services Act is the principal legislation for public sector records management in Botswana, it is weak and does not give much guidance on managing digital authentic records, except to include in its definition of a record, a definition of a digital record.
- Both the Electronic Records (Evidence) Act and the Electronic Transactions Act recognise digital records as evidence and recognise the need to promote authentic records in information systems. They both outlaw the rejection of digital records solely on the basis of being digital.
- The Cybercrime and Computer Related Crimes Act promotes the maintenance of authentic records in business systems and in this way makes it illegal for any actions that may cause the authenticity of records to be in question.
- The Criminal Procedure and Evidence Act is limited to paper records and lacks guidance on digital records, let alone how their authenticity can be ensured.

6.2.2 Procedures for the Maintenance of the Authenticity of Digital Accounting Records

The second objective of the study was to find procedures in place to maintain the authenticity of digital accounting records created and stored in GABS. The findings revealed that from the records management point of view, there are no procedures in place to ensure that once accounting records are created in GABS, they remain authentic. The records management professionals profess to use the international records management standard, ISO 15489-1, to guide records management practices. It is yet to be domesticated and there are no guidelines on how it is to be used. ICT specialists rely on both general and system application controls to maintain the authenticity of digital records in GABS. For audit purposes, auditors check the authenticity of records in GABS by instituting analytic procedures through the help of general auditing software such as ACL and IDEA. If the authenticity of records is in question during the audit process, such records are rejected.

The Office of the Auditor General of Botswana has a well laid down financial audit process that must be followed during audits. It is a step-by-step process that serves as a governing framework for the audit process. The components of the audit process include pre-engagement activities, strategic planning, detailed planning and field work, audit summary, and conclusions and reporting. Across all these stages, documentation and records are crucial as audit evidence. Authentication of records is not explicitly stated. It is implied as part of the audit process and includes a test of key controls as well as performing substantive analytical procedures.

6.2.3 Skills and Competencies for Authenticating Digital Records

The third objective of the study was to establish the skills and competencies needed by auditors, ICT specialists and Records Managers to authenticate digital records created and stored in GABS. Records management professionals have to possess skills and competencies needed to manage records in the digital environment. These include, but are not limited, to knowledge on digital preservation, computing skills, auditing, metadata, competencies to manage digital records systems, legal aspect of information, analytical and planning skills, and security and privacy control.

ICT professionals need technical competencies to be able to ascertain the authenticity of digital records created and maintained in business systems. They include skills and competencies related to system design, business process analysis, business rules, data analytics, computer forensics and security, database administration, professional IT certification (information systems auditor), IT security-related technical competencies and monitoring and evaluation of system user roles and individual logging credentials.

Auditing in the digital environment can be a mammoth task due to the complexities of modern business information systems. This makes it a requirement for auditors to possess the requisite technical skills and competencies related to computer systems. This would enable them to assess the authenticity of records in business systems. This study has revealed that they need skills and competencies such as knowledge in data analytics, business rules, and business process analysis, the use of CAATs, an understanding of system design and development, information system audit expertise, monitoring and evaluation, continuous training on GABS, as the system is continually being upgraded, presentation and creative skills. For auditors, a lack of these skills and competencies can translate into poor quality audits, wrong audit conclusions, inability to pick irregularities in financial statements, delayed audit reports and the inability to establish the authenticity of data and transactions in the system.

6.2.4 Management of Authentic Digital Records

Business systems should be able to capture business transactions with records as the evidence of such transactions. The fourth objective of the study was to determine the management and preservation as authentic and reliable to support audit processes in the public sector of Botswana.

6.2.4.1 Types of Accounting Records Captured in GABS

This study found that various financial records are created in GABS and these include, but are not limited to, records related to the functions of budgeting (e.g. commitment and expenditure records), payables (e.g. invoice registers, invoice batches, expenditure reports, payment registers, outstanding payments, listing reports), receivables (e.g. auction reports, receipts from revenue, advance overpayments, traffic fines, deduction of salary overpayments) and after spending (estimated budgeted against collected revenue, budget actual expenditure, development votes and budget against actual expenditure). In terms of the capturing of records onto the system, this is done through direct capture onto GABS or uploaded onto the system. Others are imported from other business systems that have been integrated with GABS.

6.2.4.2 Records retention and disposal in GABS

Records cannot be kept forever. They need to be disposed of after the due process of records appraisal using approved records retention and disposal schedules. This study has revealed that although the Financial Instructions and Procedures contain some records retention periods and BNARS developed a public sector-wide records retention and disposal schedule for common records, including accounting records, these have not been configured into GABS. This means that ever since the system was implemented, no records in the system have been disposed of. Such records still reside in the system as if it is in archiving, which it is not. Notably, an ECM is appropriate for records management. If GABS were integrated with one, it would cater for records retention and disposal. However, the system is not integrated with an ECM.

6.2.4.3 Preservation Strategies for Digital Accounting Records

Digital records need to be preserved as evidence of business for as long as they are needed to transact further business. Due to the ever-changing digital technologies, records produced by such systems need to be preserved, even with these changes. Records preservation strategies must be instituted to make such records accessible. This study has shown that, ever since GABS was implemented in 2004, it has been upgraded a couple of times as time passed. In order to preserve the records in the system, records preservation strategies such as migration, refreshing, technological preservation and institutional disaster planning have been preferred. A good records preservation system such as Archivematica is a useful solution that BNARS can explore to manage digital records with archival value over time. It is an open-source digital preservation system and supports long-term accessibility, authenticity and usability of digital records over space, time and technology (Garderen, Jordan, Hooten, Mumma & McLellan n.d:4). Archivematica conforms to the functional requirements for the archiving of digital data.

6.2.4.4 Integration of GABS with other Information Systems

GABS has been integrated with 17 business information systems from other government departments. None of these has record-keeping functionalities. The integration of GABS with these other systems largely focuses on the shared financial records from these systems. However, GABS have the capability to interface with record-keeping systems. For example, GABS can integrate with the Court Records Management System (CRMS), which manages digital court records in the High Courts and Magistrates Courts but that has not been done. Most records in GABS have medium-term value of up to 10 years. Some records, such as various reports generated in the system, have archival value. Integrating GABS with an ECM can help manage records in the system over time as an ECM can manage records retention and disposal. An alternative is to appraise the records, and those with archival value can be transferred to DIT data centres. BNARS does not have capacity to ingest such records into archival custody as it lacks the infrastructure to do so (Ngoepe & Keakopa 2011:157). Katuu and Ngoepe (2015:63) note that, even before the advent of cloud computing, the transfer of digital records from public institutions into archival custody has not happened in a systematic manner.

6.3 Proposed Framework

The last objective of this study was to develop a framework to authenticate records in the government accounting system in Botswana to support the audit process. A framework can be developed from research outcomes (Green 2014:35). Scholars such as Ngulube et al. (2015:10) aver that a theoretical framework assists in the interpretation of events in the world. De Benetti (2009:2) argues that theoretical frameworks are models capable of predicting future occurrences. More explicitly, theories depict relationships produced among concepts and sets of concepts, enabling an understanding of phenomena as well as providing a basis a consideration how what is unknown can be organised.

The proposed framework was developed from the study findings as presented in Chapter Four and Chapter Five, as well as the literature review presented in Chapter Two. It is intended to facilitate the financial audit process where accounting records created and stored in a business information system such as GABS can be authenticated so that they can support the audit process. It is hoped that the framework would help in the creation and maintenance of authentic digital records that are authentic and reliable enough to be acceptable in the audit process. The proposed framework was developed from the concept of archival diplomatics (Eastwood 1994:124; Duranti, Eastwood & MacNeil 2002; InterPARES 2005; Duranti 2009:52). The framework is depicted in Figure 6.1 and is explained in the sections that follow.

6.3.1 Explanation of the Proposed Framework

The framework attempts to show the link between factors that need to be in place in order to authenticate digital records for purposes of supporting the audit process. These include legislation, records management standards, auditing standards, prowess (skills), authenticity (integrity and identity of records), records retention and disposal, digital signatures, auditing software, persons, archival bond, IT and system application controls and ICT infrastructure. Figure 6.1 presents the proposed study framework to authenticate digital records in GABS. An explanation of the proposed framework is thereafter explained.

PROPOSED STUDY FRAMEWORK

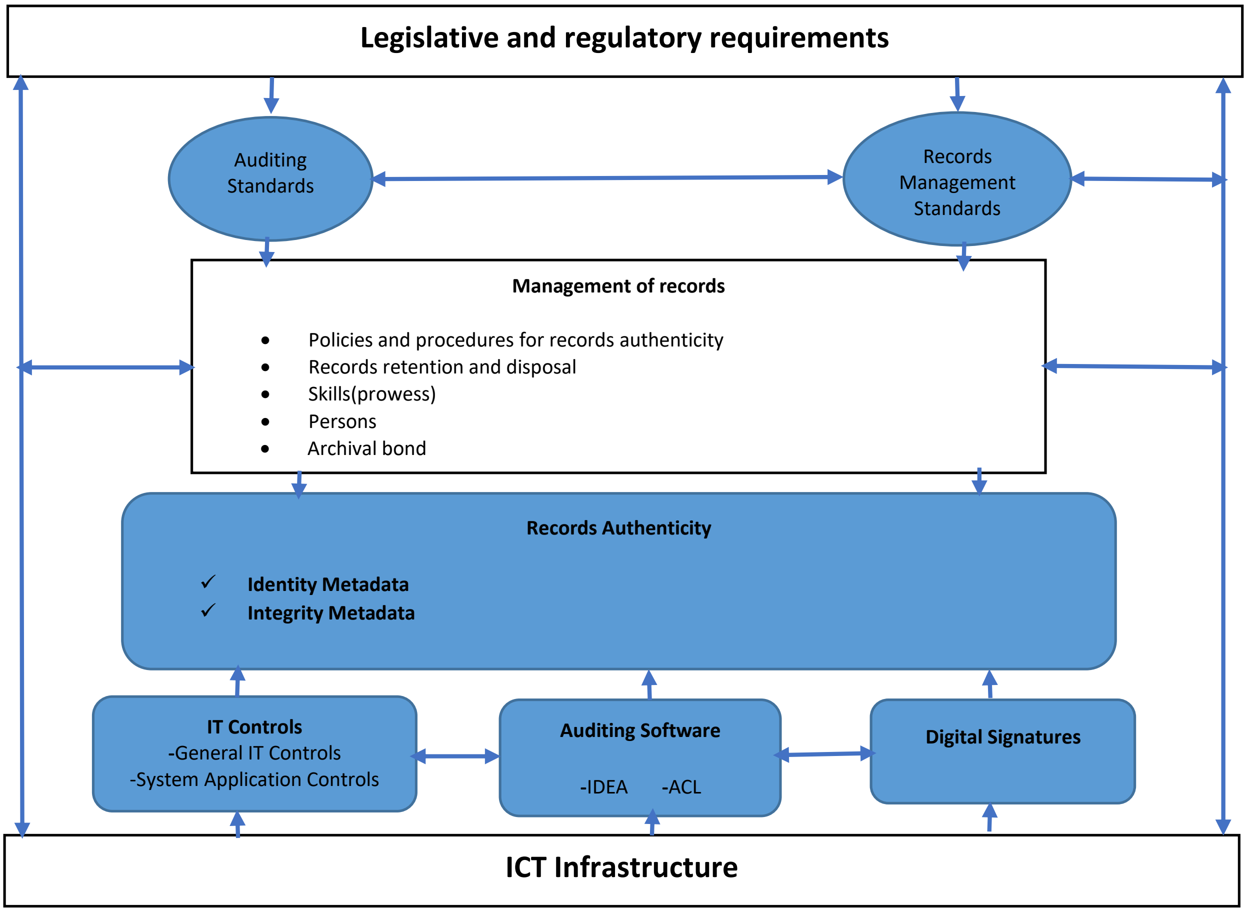


Figure 6.1: Proposed framework to authenticate digital records in GABS

a. Legislation

A framework to authentic digital records to support the audit process needs to be underpinned by appropriate legislation and auditing standards. This study has shown that both legislation and auditing standards are crucial in the financial audit process (Government of Botswana 2007; 2012; 2014a). The Electronic Records (Evidence) Act provides for the recognition of digital communications, authenticity of digital documents and admissibility of digital evidence (Keetshabe 2015). It also provides for the authentication of digital records and equates the weight of the evidence carried by digital records to that of their paper counterparts. It bars their rejection by the courts solely because they are digital (Government of Botswana 2014a). This legislation is supported by the CCRCA, which criminalises unauthorised access to computer data and systems with the intention to alter, delete or modify data, resulting in data that are inauthentic (Government of Botswana 2007). Article 7 of the Budapest Convention urges member states to criminalise all forms of computer related forgery and "...international…input, alteration, deletion, or suppression of data resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic" (Council of Europe 2001a:6). It is also the contention of the Council of Europe (2001b:9) that the most effective way of addressing issues of unauthorised access to computer systems and data is the introduction of effective security measures. In addition, the law should criminalise such acts. The Council of Europe (2001) cautions that care should be taken not to criminalise legitimate and common operating or commercial practices as the intention is to protect the confidentiality, integrity and availability of computer systems or data. A supportive legislative framework forms the foundation of a framework for the authentication of digital records.

Provisions of the Electronic Records (Evidence) Act prescribes a number of ways in which digital records can become acceptable as evidence in legal proceedings and these are as follows:

- For digital records to be accepted as evidence there is a need to prove that their production followed an approval process. The process referred to means certification of the digital records system that produced the record by the Botswana Communications Regulatory Authority (BOCRA).

- Secondly, digital signatures can be used to verify the authenticity of the record.
- Thirdly, the integrity of the record needs to pass the best evidence rule such that there will be no doubt that the record is authentic.
- There should be no doubt regarding the accuracy of the digital record due to improper use of the digital records system that created and stored it.
- The record should also have been created and stored in the normal course of business (Government of Botswana 2014).

The Electronic Communications and Transactions Act (ECT Act) (Government of Botswana 2014) also has provisions that support the creation and maintenance of authentic digital records. Digital signatures are acceptable to authenticate digital records and their validity or enforceability is not to be rejected solely because they are digital. For the digital signature to be deemed reliable, its creation data should only be linked to the person whom it was assigned to. Digital records are also to be trusted to be authentic if it can be proved that they have not been modified after the reason for their generation. The Act prescribes that, if there is reasonable doubt about the reliability of digital records, they should be assessed for integrity. The assessment for such integrity should be about ensuring that no alterations were made to the record besides any additions made in the normal course of business, its storage, display and the principal reasons why the was generated in the first place.

b. Auditing standards

Apart from appropriate legislation, auditing standards are crucial in the endeavour to promote the authentication of digital records to support the audit process. It has also been shown in this study that the PAA regulates financial auditing in the public sector (Government of Botswana 2007). It empowers the Auditor General to adopt standards and other necessary tools for implementing the auditing standards such as the ones issued by the International Auditing and Assurance Standards Board (IAASB) in the audit process. The International Auditing Practice

Statement 1013 requires that when planning audits, auditors should obtain a general understanding of the legal and regulatory framework applicable to the entity audited and the state of compliance of the entity with the framework (IFAC 2010:225). The same auditing standard puts emphasis on risk identification during the audit process. These risks may be related to:

- loss of transaction integrity, the effects of which may be compounded by the lack of an adequate audit trail in either paper or digital form
- pervasive e-commerce security risks, including virus attacks and the potential for the entity to suffer fraud by customers, employees and others through unauthorised access (IFAC 2010:223).

ISA 250 also recognises that in the context of laws and regulations, the auditor should understand the legislation that affects the operations of the auditee and they relate to auditing of financial statements (IAASB 2010:201). This is because non-compliance with such laws and regulations may involve conduct meant to hide wrongdoing that may include collusion, forgery and deliberate failure to document transactions, management override of controls or intentional misrepresentations being made to the auditor.

Although the standards may not have prescriptions for the creation and maintenance of authentic audit evidence (records), it is a fact that auditors rely on authentic records to support audit processes (Ngoepe 2004:8; Ngoepe & Ngulube 2014:142). The International Records Management Trust (2003:2) reports that, in Nigeria, auditing experienced problems and these were associated with record keeping, specifically issues of non-compliance with procedures for contract administration, insufficient documentation supporting purchases, incomplete reconciliation, failure to account properly for stores and weaknesses in documentation. All these provide a fertile ground for fraud.

c. Adoption of appropriate standards in archives and records management

This study has revealed that neither international best practices in archives and records management nor local ones (none exist) have been adopted by BNARS to guide the management of digital records in the Botswana public sector. According to Seymour (2016:35), to control digital records, there is need for standardisation. It enables the capturing and preservation of original records and evidence of access or changes made to them. Records management standards promote the creation of authentic records. The standards can be adapted and customised to the local environment. These standards include the following:

- ISO 15489-1 (2016): Information and documentation – Records management – Part 1: Concepts and principles
- ISO 15836: 2009: Information and documentation – The Dublin Core metadata element set
- ISO 23081-1: 2006: Information and documentation – Records management processes Metadata for records: Part 1: Principles.
- ISO 16175-2: 2011: Information and documentation – Principles and functional requirements for records in electronic office environments: Part 2: Guidelines and functional requirements for digital records management systems.
- The Australian Government Recordkeeping Metadata Standard version 2.0 (AGRkMS). The standard recognises that authentic records satisfy the need for records to be accepted as evidence of business transactions and that is identified in the metadata such as date range, record-keeping event name: migrates and document form name: digital signature (Tennis & Rogers 2012:39).
- IRMT best practice guidance tool on Integrating Records Management in ICT systems: Good Practice Indicators (IRMT 2008).

d. Authenticity (records integrity and identity)

In archival diplomatics, authentic records are those records whose integrity can be demonstrated and identity established (Duranti & Blanchette 2004:2; InterPARES 2008:731;

Rogers 2015c:101). To protect the authenticity of records in GABS, it is important that their identity and integrity metadata is in place (Duranti 2014). Metadata is central to the authentication of digital records (Wallace 2000:3). The metadata should be related to the records' content, structure and context as professed by Bearman (2007:18). Metadata can be descriptive, structural and responsible for the preservation of information resources (NISO 2004:1; IRMT 2008:66). According to IRMT (2008:6-8), for records to make sense, their content should be linked to its structure and context. The context can be legal-administrative, provenancial, procedural, documentary and technical and, in this sense, metadata helps to document the reliability and authenticity of records and record-keeping systems (InterPARES 2008:1). The very same metadata ensures that records are identifiable and can be managed, stored, used and reassembled to generate an authentic copy of a record (InterPARES 2008:1). Thus, through metadata, information resources can survive and continue to be accessible into the future.

e. Skills (prowess)

This study has revealed that managing digital records needs skills. Many studies done in Africa have revealed a lack of competencies to manage digital records (Mnjama & Wamukoya 2007:279; Kemoni 2009:194; Luyombya 2010:61; Asogwa 2013:799). This is a general human resource problem. The use of ICTs to transact e-government services has seen accounting functions being computerised. In the context of this study, skills needed to manage digital accounting records are needed by Accountants, as they are the ones who manage records in GABS, as opposed to records management professionals.

The highly complex environment in which computerised accounting systems are obtained has meant that auditing techniques known as CAATs have become a common feature in the workplace (Elefterie & Badea 2017:4). To audit in the digital environment, it has been revealed by this study that auditors need skills related to digital records management (including an appreciation of digital signatures), data analytics, analytical and planning skills, security of records, metadata and effective communication and consensus-building skills. These skills and competencies would enable them to be able to authenticate digital records as they conduct an audit engagement. It is particularly crucial for auditors to develop technical skills needed for auditing in the networked environment. They need knowledge, competencies and content of the IT subject areas such as:

- IT systems for financial accounting and reporting, including relevant current issues and developments
- principles and practices for evaluating financial accounting and reporting systems, including evaluating controls and assessing risk
- computer-assisted auditing packages and techniques (International Federation of Accountants 2005:15)

ICT specialists also need to have technical skills, which they can use to ensure that system supplication controls and general controls of an information system are working properly. The specific skills cited in this study include database administration, system design, metadata, data analytics, business process analysis, IT Certification (information systems auditor), IT security-related technical competencies as well as computer forensics and security. These skills and competencies are crucial for the authentication of records. The Digital Continuity Strategy of the National Archives of Australia affirms that ICT professionals need skills and competencies to equip them to manage digital information, including records (National Archives of Australia 2015:3-10). Knight (2010) carried out a survey on ICT attitudes to records and record keeping, and the ICT professionals indicated that they needed skills related to the following:

- Devising strategies for ensuring the long-term accessibility and usability of digital information.
- Contributing records requirements to systems design and implementation.
- Defining digital records and differentiating these from other kinds of digital information.
- Ensuring that required records are not lost in migrations.

- Retention of digital records.

Both auditors, records management professionals (Accountants who manage records in GABS) and ICT professionals need different sets of skills and competencies that they can use for the authentication of digital records. Personnel who manage digital records need to have a defined minimum skill sets and competencies for their management (Ambira 2016:345).

f. Management of records

Records, regardless of their format, records need to be managed properly for the benefit of the organisation that created them. Aspects of records management such as policies and procedures, and records retention and disposal scheduling have emerged in this study as crucial in the endeavour to manage digital records that are authentic.

g. Policies and procedures for creating and maintaining authentic records

The study has also revealed that, although GABS has been implemented in government ministries and departments since 2004, there are no documented policies and procedures geared towards providing guidance on the management of authentic digital accounting records produced and stored in the system. Studies by Moloi (2009:113), Keakopa (2010:64), Ngoepe, and Keakopa (2011:155) have also shown that there is a lack of policies for the management of digital records in Botswana’s public sector. This state of affairs is actually common in the ESARBICA region, with the exception of South Africa (Keakopa 2010:63; Katuu 2016:122-123; Ngoepe and Saurombe 2016:29-37). Just like the National Archives of Zimbabwe (2018), BNARS can take the lead by providing a framework for the management of authentic digital records in the form of issuing policies and guidelines for the management of public sector digital records. Policies and framework are a necessary part of the framework for the authentication of digital records. National archival agencies such as those in South Africa and Namibia have issued policies and procedures to guide the management of digital records in their jurisdiction (National Archives of Namibia 2007; National Archives of South Africa 2007).

h. Records retention and disposal

The purpose of a records retention and disposal schedule is to control records disposal in an accountable manner (Ngoepe & Van Der Walt 2010:98). This study has revealed that ever since GABS was implemented 2004, records in the system have not been disposed of. The records have been residing in the system as if it is an archival system, although it is not. Many countries face many challenges when it comes to the long-term preservation of digital records (Keakopa 2007:33; Bearman 2007). The long-term preservation of digital records remains an unresolved problem due to the impact of ICTs on record keeping (Keakopa 2007:33). According to Duranti (2010:80), the trouble with digital systems lies in their ability to create and maintain reliable records that are preserved authentically over time without concerns over the loss of their authenticity. They can be easily tampered with and corrupted.

This raises the issue whether those records that have been residing in GABS since it was implemented in 2004 are still authentic since they were last set aside to conduct organisational business. They may or may not be authentic. This brings the issue of the importance of records retention and disposal to support the audit process. This process ensures that records are available when needed, as records without continuing value are destroyed while those possessing continuing value are preserved as corporate memory and evidence of business transactions conducted. Mojapelo (2017:31) imagines a scenario where an auditor walks into the auditee's office to undertake an audit assignment only to be told that evidence for transactions conducted in that particular period was not available because records have been destroyed. In such a situation, it would not be possible to continue with the audit or even give an opinion because of a lack of supporting documentation for transactions done. Both David (2017:13) and Okello-Obura (2012:37-38) have affirmed the centrality of evidence (records) in the audit process. Inconsistent and inadequate records management practices in Zimbabwean government entities contributed to adverse and qualified opinions and, in some cases, unqualified opinions.

BNARS has developed a records retention schedule for financial records and this can be configured into GABS in order to use it to control the accumulation of digital records. Should some records need to be destroyed, the schedule can be used to guide the appraisal of such records. With digital records, the process of appraisal (though forever controversial and yet to be standardised) appears at the centre and front of the records creation and maintenance processes (Duranti 2010:86). This is an advantage for accounting records in GABS to be earmarked for the appropriate disposal decision right from creation. Controlled records retention and disposal help to ensure that records remain available when needed to provide evidence in the audit process.

i. ICT Infrastructure

For digital records to remain authentic after creation, the ICT infrastructure has to be resilient. Although ICT infrastructure does not entirely solve problems related to the management of digital records, its availability is key to the adaptation of digital systems. ICT tools enable records creation, captures, storage and preservation processes (Muchaonyerwa & Khayundi 2014:45). The Government of Botswana has a fairly well-developed local area network (LAN) across government ministries and departments (Moloi 2009:119). An earlier study of e-records readiness in the ESARBICA region by Wato (2006:78) had shown that Botswana has a moderately developed ICT infrastructure to support the management of authentic records. The infrastructure through which GABS runs is interoperable with other business systems, including some ECMs. A harmonisation of ICT infrastructures across e-government platforms is paramount in order to ensure that they operate at the same level to achieve operational resilience and economy in a digital records management and e-government environment. This integration would include both hardware and software harmonisation. The standardisation of nomenclature for describing records within e-government, digital records and business systems needs to be done to allow seamless exchange of data using the linked database fields, but without causing any harm to the integrity and identity of records in GABS. A sound ICT infrastructure is a necessity for ensuring that business systems such as GABS are supported in the creation and maintenance of authentic records. This is also necessary for the Government of Botswana's e-government programme. The ICT infrastructure in the public sector, an enterprise-wide system known as the Government Data Network (GDN) provides the "basic technology platform for the rollout of e-Government services" (Botswana Government 2011:8). A study on enterprise-wide systems for digital records management also concluded that Botswana possesses a good ICT infrastructure (InterPARES 2017:28). Furthermore, there is reliable electricity supply, telephone and internet connectivity, computer networks and technical support provided by ICT specialists stationed in all ministries (Moloi 2009:119). The LAN is connected to the GDN for national systems such as GABS.

j. Digital signatures

There is a need for proper procedures and mechanisms in order to ensure security, long-term preservation and accessibility of digital records for effective e-governance. Challenges to records security include possible data corruption whereby the integrity and reliability of digital records are compromised (Muchaonyerwa 2017:63-64). Digital signatures are one of the mechanisms employed to authenticate records. Digital signatures consist of information that is attached to a record or is logically associated with a record. It is used as a method of authentication (European Commission 2008:124). It is typically a sequence of characters and is "secured with algorithms, procedures and "keys" (a long string of characters analogous to a password) to confirm the integrity of a record, and/or to authenticate the identity of the sender or the source of a record." According to the Centre for Technology in Government (2003:2),

> A digital signature is an unforgeable piece of data, which asserts that a certain person either wrote or otherwise agreed to the digital document to which the digital signature is attached. The recipient of a digitally signed electronic document can verify both that this document came from the person whose digital signature is attached and that this document is not altered after it is signed.

A digital signature guarantees that no alteration and variations are made to digital records without detection. Thus it provides added assurances of evidence to the origin, identity and status of a digital document, transaction and acknowledgement of informed consent by the signer. The use of digital signatures for authenticating digital records helps to reduce fraud and detects forgery or tampering with records (Oloyede 2017). Digital signatures are thus an integral part of the proposed framework to authenticate digital records created and stored in GABS. As a method of authentication, the digital signature is allowed in the Electronic Communications and Transactions Act (Government of Botswana 2014).

k. IT and system application controls

IT and system application controls are crucial in ensuring that records in computer-based information systems are protected. It has been revealed in this study that general IT and system application controls are used to protect the authenticity of records in GABS. It is therefore befitting that these be included in the proposed framework to authenticate digital records in GABS. These controls are technical and social (Rogers 2015b:95). Technical indicators of records authenticity such as audit logs/trail, metadata, deployment of software to monitor the activities of system administrators, access controls to systems and access controls to computers need to be maintained all the time, as social indicators of authenticity need to be considered to attest records authenticity (Rogers 2015c:106). They include policies and guidelines to protect the authenticity of digital records, system documentation on segregation of duties in the system and documentation of authorisation to use the system. The security of records in e-government systems such as GABS is crucial as it ensures that records retain their authenticity. Security features of the GABS system application and general IT control levels are a requirement. Mechanisms for authentication ensure that data and records are used to facilitate the consumption of services not based on forged or fraudulent records. Technical measures to attest to records authenticity are supported by both the Electronic Communications and Transactions Act and the Electronic Records (Evidence) Act.

l. Archival bond

Transactions in GABS are related to others within and outside the system and, consequently, create records as evidence of the same transactions. At the start of every financial year, a budget is prepared and captured into the system. Expenditure is then monitored against the budget as approved by Parliament. Then, once the budget is approved, it is captured into the system. Functions performed through GABS are classified into activities and transactions that produce actual records, all these are regulated by rules of procedures and manifested through repeated actions following a certain business process (Herrera 2011:39). Thus, records in GABS have an archival bond.

The key to the existence of digital records is the archival bond (Duranti & MacNeil 1996:53). Archival bond refers to the relationship that links each record to the previous one and the subsequent one (Duranti 2001:273). An archival bond is created once a record is set aside to transact a business function and may be manifested in a classification code assigned to the record in a grouping of records belonging to the same class. This is also obtained when records are registered (incoming or outgoing) and assigned registration numbers (Duranti & MacNeil 1996:53). Notably, in business systems without record-keeping functionalities, the classification code or filing identifier and, if applicable, registration number are part of the metadata which constitute the data dictionary (Duranti & MacNeil 1996:54). Archival bond is the same concept of interrelatedness in the view of Eastwood (1994:128) who refers to it as "functional and structural bonds that bind the documents together in a whole whose integrity is important to their meaning, significance, and value as evidence." Duranti (1997:217) who observes that during migration of data between information systems, it is probably the best method for ensuring the authenticity of digital records in the long term, underscores the importance of the archival bond.

m. Persons

Persons authorised to transact business functions create records. Archival diplomatics theories state that a digital has eight components, of which ‘persons’ is one (Duranti 2001:44). These are the four persons involved and they comprise the entities transacting business by means of the record: author, addressee, writer and creator. Duranti and MacNeil (1996:51-52) note that while these many persons take part in the creation of a record (inclusive of witnesses and countersigners), only three persons are necessary for its existence. These are the author (has authority and capacity to issue the record or it can be issued in their name), addressee (person to whom the record is directed or intended) and the writer (the person having the authority and capacity to articulate the content of the record). This then means that records creation in GABS is controlled and persons participating in the production of digital records are assigned particular roles and responsibilities. There are preparing officers, revenue collectors and authorising officers. This assignment of roles in the system is meant to ensure that only authorised personnel gain access into the system to transact business. These persons include accountants who are the day-to-day users of the system and senior officers who authorise transactions. Thus, identifiable persons in the creation of digital records fit in well with records identity and are part contributors to the creation of authentic records as theorised by archival diplomatics.

n. Auditing software

The use of audit software is unavoidable in an era where ICTs have been used to aid delivery of services to business and citizens (Public Records Office 2001:2). ICTs have been used to meet the expectations of users of financial and other business performance information (Ahmed 2003:20). This study has revealed that auditors use audit software, generally referred to as CAATs to verify the authenticity of records in GABS during the audit process. internal auditors from the Department of Internal Audit (DIA) used ACL auditing software while external auditors from the Office of the Auditor General of Botswana use Interactive Data Extraction and Analysis tool (IDEA) audit software. Audit software can, among others, confirm the correctness of calculations or the lack thereof, confirm whether the relationships between data items are correct or not, spot inconsistencies in data relationships, identify unusual or unexpected transactions (e.g. large journal postings, transactions entered at unusual times) and investigate whether programmes are performing as expected following set business rules (Lewis 2009:6-7). All these point to the fact that CAATs can be used to verify the integrity of data in business systems in the financial audit process.

6.4 Conclusions of the Study

The conclusions of the study are based on the research objectives. Babbie (2004:490) avers that "the report should conclude with the statement of what you have discovered about your subject matter and where future research might be directed". According to the University of Southern California (2018), the purpose of the conclusion is to assist the reader to understand why the research should matter after they have finished reading it. If it is well written, it provides an opportunity to demonstrate to the reader an understanding of the research problem. Based on the findings of the study, the following are the conclusions derived from the study.

6.4.1 Conclusion on the Legislative Framework for Digital Records Management

A legislative framework is crucial to guide records, regardless of form or media. Laws are meant to guide records management practices as well as appropriate business process. In this case, this refers to auditing and financial management. An analysis of the legislative framework shows that there are relevant laws to regulate public sector records management as well an audit of government financial statements.

The principal law governing public sector records management establishes BNARS and outlines the roles and responsibilities of the Director of the department. The Act also stipulates the mandate of the department, which is archives and records management services, which include the management of digital records. However, the Act does not prescribe measures necessary for the maintenance of the authenticity of digital records produced in information systems implemented in the public sector. Furthermore, the department has not issued and shared guidelines or standards to be observed by government departments, although many of them have implemented information systems and these produce digital records.

Despite the weaknesses of the National Archives and Records Services Act of 1978 (amended in 2007), all is not lost, as three laws (the Electronic Records (Evidence) Act, the Electronic Transactions Act and the Cybercrime and Computer Related Crimes Act) have provisions to protect the authenticity of digital records produced by various business systems implemented in the public sector. The Electronic Records (Evidence) Act provides for the authentication of digital records. The digital records are acceptable as evidence in a court of law in a similar way as their paper counterparts, as long as it can be proved that they are authentic and can thus stand for the facts that they attest. As evidence, the digital record carries the same weight as its paper counterpart and cannot be thrown out by the court because it exists in digital form.

The Electronic Communications and Transactions Act facilitates and regulates digital communications and transactions, specifically digital commerce and digital signatures. The Government of Botswana promotes and participates in e-government transactions. The Act gives legal recognition of both internal and external digital transactions, which produce digital records. As long as the digital records arising from e-commerce transactions can be proved to be authentic and reliable using digital signatures (both local and foreign), the records would be accepted as evidence by the courts. The digital signatures conform to international standards in terms of reliability and security.

Two other Acts are crucial in the auditing and public finance management. These are the PAA and the PFMA. The PAA mandates the Auditor General of Botswana to conduct an annual financial audit of public sector agencies. The financial audit process results in an audit opinion, which is based on records. Records management requirements in the audit process are not specified although, in practice, financial auditing relies heavily on records. These requirements are implicit. Therefore, it does not come as a surprise that the Act does not offer any guidance on the records authenticity requirements necessary for the acceptance of digital records in the audit process. It is notable that the Act promotes compliance with auditing standards as issued by the International Auditing and Assurance Standards Board (IAASB) in the audit process. The standards do not offer guidance on how to ensure the authenticity of records (audit evidence) consulted during the audit process, although they infer that audit evidence is central to the audit process.

The PFMA prescribes that annual financial statements should be prepared by the Accountant General, a government officer within the MFED. These have to be made available to the Auditor General to perform a financial audit that has to be presented to Parliament by the Minister of Finance and Economic Development. This Act promotes accountability in the use of financial resources at the beginning of every financial year. Since this Act is crucial in the audit process, which utilises records as evidence, it indirectly supports good records management practices by government ministries and departments. This piece of legislation implicitly promotes the proper management of accounting records as they are used in the audit process. However, it does not provide guidelines on the creation and maintenance of authentic records as produced in GABS. It is technology neutral and, although it regulates auditing in both the digital and physical environment, does not say anything about the need to create and maintain authentic records.

6.4.2 Conclusions on Procedures to Maintain Records Authenticity

In the context of this study, records authenticity is a key concept for archives and records management professionals, ICT professionals and auditors, both external and internal. Firstly, this study has revealed that GABS, as a business system, produces digital accounting records. This is shown by the system ticking all the boxes when evaluated against InterPARES (2002) Benchmark Requirements Supporting the Presumption of Authenticity of Digital Records. The benchmark was used as an evaluation tool to assess the capability of GABS to produce truly digital records as theorised by archival diplomatics.

Concerning records authenticity needs for archives and records management professionals, this study concludes that BNARS, as a department mandated to coordinate public sector records management initiatives, has not provided any guidelines on how government ministries and departments implementing record keeping and/or information systems that produce records can maintain the authenticity of records once created. There are simply no procedures in place. This includes standards for records management. Secondly, it has become clear that records management professionals lack awareness of digital records management issues in general and authenticity of digital records in particular.

For ICT professionals, they use social and technical indicators to check and maintain the authenticity of accounting records in GABS. These are the general computer controls and system or application controls. These controls include segregation of duties, read only status of records (no cancellation), inbuilt computer security mechanisms, usernames and passwords, audit trails, policy on information security and controlled physical access into server rooms.

Auditors also care about records authenticity. They rely on authentic records during the audit process. This study has revealed that auditors verify the authenticity of records in GABS during financial audits, as they use CAATs to facilitate the audit process. Internal auditors from the Department of Internal Audit within the MFED use ACL software, while external auditors from the Office of Auditor General of Botswana use IDEA software for auditing. The software is used to perform analytical procedures, and these are able to pinpoint errors, inaccuracies in financial statements. These can suggest inauthentic and thus unreliable records and, if that is the case, the records are rejected in the audit process. Auditors at the Office of Auditor General of Botswana follow a well laid down audit process from their initial contact until their issuing of an audit report with an opinion on the state of finances. The auditors also follow international auditing standards.

6.4.3 Conclusions on Skills and Competencies for Authenticating Digital Records

The management of digital records, including the maintenance of their authenticity, requires personnel with the requisite skills competencies. The same is true for auditors who audit financial statements in the digital environment. This indicates that archives and records management professionals need skills and competencies, especially technical ones such as metadata and auditing, digital preservation competencies, digital signatures and digital records management skills and competencies. This study has revealed that records management professionals lack computing skills and competencies to enable them to manage digital records and ascertain their authenticity. A lack of capacity to manage digital records by records management professionals has dire consequences, which include poor preservation of records, inability to advise on digital records management, unspotted fraudulent activities and they would be ill equipped to authenticate digital records.

ICT professionals also need to be equipped with up-to-date skills and competencies to enable them to manage databases and uphold the identity and integrity of records in GABS. This study has revealed that ICT professionals possess the requisite skills and competencies needed to support GABS and maintain the authenticity of records in its database. Secondly, it became clear that they still need refresher courses to keep up to date with the ever-changing technologies. Mostly, they use both social and technical controls to maintain the authenticity of accounting records created and stored in the GABS database. They voiced that a lack of computing skills would nullify their capabilities to spot anomalies in records in the database. System security would be compromised, unspotted access to the system can occur and even accidental deletion of data in the system. It is of paramount importance for ICT professionals to have the requisite skills and competencies. Lack of such skills would lead to compromised system security, unauthorised access to system as well as both deliberate and accidental deletion of data without trace being noticed.

Like records management and ICT professionals, auditors need to be prepared to undertake financial auditing in the digital environment. Some auditors in this study are accountants by training, while others are Information Systems/ICT professionals by training. Computerised auditing, occasioned by the use of application software to manage accounting transactions, and has meant that auditors who are accountants by profession need skills and competencies to do their work in a computerised environment. This study has shown that these auditors are well equipped to start and finish audit assignments in the digital space. The skills include data analytics, knowledge and use of CAATs, business process analysis as well as an understanding of system design and development. Such skills and competencies have enabled them to check and verify the authenticity in GABS and their state of affairs with regard to their acceptability in the audit process. If the authenticity of the digital records are suspect, they are rejected as evidence in the audit process. Although the auditors are well equipped to deal with the audit assignment in the virtual environment, it emerged that they need continuous education and development in order to keep abreast with developments in ICTs. If auditors are not capacitated enough to work with ICTs, they would not be able to authenticate digital records; they would use unreliable and inauthentic records in the audit process; they would be unable to spot incorrect data and they would end up issuing audit reports based on fraudulent data.

6.4.4 Conclusions on the Management of Authentic Digital Records

Just like manual records, digital records need to be managed beyond their use by the creating agency. This study shows that GABS creates and stores accounting records in line with the accounting and budgetary process. The records are either captured directly onto the system, uploaded or imported from other systems that interface with it. These records reside in the system such that GABS act more like an archiving system. It is notable that records retention and disposal schedules have been developed by both the AGD, as in Financial Instructions and Procedures, and the BNARS. However, they have not been configured into GABS. Since 2004 when the system was configured, records have been residing in the system. Records managers based at the MFED are not aware of the developed schedules. ICT professionals, on the other hand, are aware of the schedule from the Financial Instructions and Procedures.

The preservation of records in GABS has been done through strategies such as migration, refreshing and technological preservation. These are the strategies put forward by ICT professionals. Records managers, on the other hand, are not aware of any strategies because they do not use digital accounting records. Some opined that the DIT is responsible for digital preservation of records although the department is only mandated to provide the infrastructure required for digital preservation. In terms of integration with other business systems, GABS is robust enough to interface with many systems from other government departments largely for accounting and finance management transactions.

6.5 Recommendations

This section of the study suggests recommendations to issues identified in the study. The recommendations are based on the findings of the study in line with the study objectives.

6.5.1 Analysis of the Legislative Framework for the Creation of Authentic Digital Records

This study has found that archival legislation in Botswana is weak and does not lend itself to providing guidance for the management of digital records. To use the words of Ngoepe and Saurombe (2016:37), the legislation was clearly enacted principally with paper records in mind; hence, its focus on such records types. There are provisions for the management of authentic digital records in other legislation such as Electronic Records (Evidence) Act, Electronic Transactions Act and the Cybercrime and Computer Related Crimes. In this context, the following are recommended:

- The National Archives and Records Services Act should be amended to make it comprehensive enough to make specific provision for the management of digital records in networked environments.
- The specific areas could include defining a digital record specifically, instead of relying on a broad definition of a record.
- The BNARS should develop specific guidelines for the appraisal of digital records.

- BNARS should be involved in the procurement of information systems that create public records so that records management functionalities are made part of the design of such digital systems from inception.
- The department should also provide guidelines for the creation and maintenance of authentic reliable digital records created in different systems to be used by government ministries and departments since it does not have the infrastructure to ingest digital records transferred from such entities.
- Since BNARS lacks capacity for digital records management, it is recommended that such capacity be built through staff attachment at established archival institutions that have mature digital records management programmes.
- BNARS should domesticate international records management standards that guide digital records management, implement them and monitor their implementation in government ministries and departments.
- BNARS should mount an awareness-raising campaign on digital records management issues geared towards public sector records management professionals and government ministries and departments.
- BNARS should collaborate with stakeholders such as organisations with digital records preservation capabilities, ICT professionals, legal practitioners, educators and auditors in developing a digital records strategy capable of facilitating the acceptance of digital records in the audit process.
- BNARS is also encouraged to play an active role in issues of open data and big data initiatives. This is apparent as according to Thurston (2012), the success of Open Government (both of proactive disclosure (Open Data) and reactive disclosure (Freedom of Information/ Right to Information) rests ultimately on the governments' ability to create and maintain reliable, trustworthy and accurate information (records and data) and on people's ability to access it

6.5.2 Procedures in Place to Maintain the Authenticity of Digital Accounting Records

This study has revealed that auditors and ICT professionals use different methods to authenticate digital records. ICT professionals use both technical and social indicators of records authenticity. Auditors use CAATs to verify the authenticity of records in digital systems. The following recommendations are put forward in order to uphold the authenticity of records in digital systems:

- Internal controls (application controls) and monitoring of transactions in GABS need to be improved. Starting from the designing of systems, all stakeholders should be involved to ensure that the system has adequate, effective and efficient internal controls. After implementation of the system, system controls should be reviewed to ascertain the effectiveness.
- The disaster contingency site should be far enough from the production system (e.g. in a different city).
- A data warehouse should be built to house old records that currently sit in the system.
- Technology solutions should be implemented to monitor activities of database administrators and system administrators.
- Authorisations for all transactions should be performed on the system for efficient tracking.
- There should be no or very little human interference in the processing of records, except maybe at capturing stage only

6.5.3 Skills and Competencies Needed by Auditors, ICT Specialists and Records Managers to Authenticate Digital Records

It has been revealed in this study that although records management professionals, ICT professionals and auditors have been trained to perform their work functions, it is necessary to continue equipping them with skills and competencies in order for them to continue to operate effectively in the face of the ever-changing technologies. This would enable them to continue being able to authenticate records in digital systems, including for auditing purposes. In view of the aforementioned, this study recommends the following:

- Internal auditors should be trained more in internal audit processes and techniques as they have accounting qualifications not internal audit ones.
- Internal auditors should be capacitated so that they are COBIT certified, Oracle certified and ACL certified.
- There is need for continuous on-the-job training on performing data analytics using auditing software and computer information systems.
- Proper and relevant training should be availed to programmers in order to enable them to produce what is communicated to auditors.
- Regular and continuous GABS system training should be made available to auditors.
- BNARS should promote deliberate and continuous dialogue, engagement and empowerment of records managers on public sector digital records management issues through workshops, conferences, seminars and best practice international benchmarking visits to those who have made strides on management of digital records.
- Records Managers must be trained in financial records so that they grasp issues related to managing computerised financial records.
- Archives and records management professionals should receive continuous training in digital records management. BNARS should instigate a public sector-wide skills gap on the management of digital records among the Records Managers and Archivists.

6.5.4 Management of Authentic Digital Records to Support the Audit Process

This study has determined that financial transactions done through GABS produce digital accounting records and these are stored in the system. It has also emerged that GABS has the capability to be integrated with true record-keeping systems, but this has not been done and such systems have been implemented. Another finding has been that although records retention and disposal schedules for accounting records either through the Financial Instructions and Procedures and the Generic Records Retention Schedule have been developed by BNARS, these have not been configured into the system. Other than that, the study has revealed that there is low awareness of digital records management among records management professionals and there are no policies and guidelines to guide digital records management. Therefore, this study offers the following recommendations to improve digital records management and the preservation of such records:

- GABS is a robust business system that can interface with many other information systems. The study recommends the integration of GABS with digital records management systems where they have been implemented such as the Court Records Management System (Administration of Justice's Magistrates Court and the High Courts) and the Document Workflow Management System (Ministry of Investment, Trade and Industry). This calls for BNARS to be proactive and show direction when records management systems are implemented in the public sector. Integrating GABS with digital records management systems would ensure availability of financial records, especially when such systems have a module on managing financial records.
- BNARS should develop and implement a National Records Management Policy on digital records management. The policy would provide a general framework for guiding digital records management in the public sector.
- BNARS should also develop, implement and monitor compliance with guidelines that would provide specific guidance to various facets of digital records management such as social media records management in the public sector and managing e-mail as records.
- Backup data for GABS are stored in the two data centres located within the offices housing the DIT (Blocks 6 and 8 in the Government Enclave). It is possible to lose vital financial records in the event of a disaster affecting these two buildings. It is recommended that a data centre for the archiving and storage of data from GABS be located outside the city of Gaborone in order to minimise loss of data in case disaster strikes.

6.6 Further Research

As shown in Chapter 1, section 1.10, a research study has a scope and cannot cover all grounds. This study has revealed that the audit process requires authentic records or else they are not accepted as audit evidence. It has also shown that the legislative framework does support the creation and maintenance of authentic reliable digital records although in practice there are shortcomings in the principal archival legislation. Furthermore, there is an absence of guidelines on the day-to-day management of digital records. It has also revealed that auditors need skills, competencies, and Records Managers for them to authenticate records created and stored in GABS. Lastly, the study found that there are efforts to preservation strategies that are employed to manage records in GABS. Further areas worth looking into by other researchers are suggested as follows:

- The principal archival legislation in Botswana is weak and is not capable of guiding digital records management in the country. A study that investigates the consequences of inadequate archival legislation on public sector records management practices is desirable.
- Another study could be conducted with a focus on the role of auditing in promoting records management provision since that angle was not covered by the current study.
- Another possible area, which could be explored by a future study, could be the role played by proper records management programmes in aiding the audit process. The study could be a public sector-wide study using a survey methodology.
- This study has revealed that computerised accounting records are managed by Accountants and not by records management professionals. Accountants lack records management capabilities both in the manual and digital world. A study of records management capability requirements by Accountants for effective management of computerised accounting records is feasible.
- This study has revealed that archives and records management professionals lack skills and competencies in digital records management. A government-wide study on records

management capabilities for digital continuity is worth looking into from the perspective of public sector records management and spearheaded by BNARS.

- This study has shown that creating and maintaining authentic digital records is an activity that needs the collaboration of records management professionals and ICT experts. A study that investigates the benefits of collaboration by archives and records management professionals and ICT experts in the management of digital records management is recommended.
- GABS is a robust business system that creates digital records. It has also been integrated with other business systems and can be interfaced with dedicated record-keeping systems. One possible area of study could be an investigation into the requirements for integrating business systems into record-keeping systems with a focus on how such an integration may affect the authenticity of digital records in business systems.
- This study has revealed instances of challenges related to digital records preservation. Since that was beyond the scope of this study, a future study on the management of digital records produced and stored in business systems can be carried out to find out solutions.
- Lastly, this study revealed that GABS can be integrated with ECMs, but that has not been done yet. This study recommends the integration of GABS with an ECM for the management of digital records be undertaken.

6.7 Implications on Theory and Practice

Research findings should be useful and connected to the bigger picture in some way, that is, to what people already know or believe about the topic in question (Leedy & Ormrod 2010:285). The empirical findings have shown that in the financial audit process, auditors rely on authentic records in the audit assignment. Furthermore, the findings have shown that procedures for the authentication of digital records in GABS are a necessity to declare such records authentic for them to become acceptable in the audit process. If the MFED adopts the study recommendations, it can collaborate with BNARS as the lead agency to develop public sector-wide procedures to guide public bodies in creating authentic records produced in various implemented information systems, including GABS. Theoretically, this study has proposed a framework to guide the authentication of digital records in GABS, a business system in the context of the Botswana public sector. This is particularly important because Botswana is a player in e-government. The framework could be extended to other contexts as well.

6.8 Final Conclusion

This study is organised into six chapters. The first one presented the context of the study, including the problem. The second one reviewed literature related to the study with research objectives serving as the main theme for the review. Chapter Three focused on the research methodology adopted for the study, including data collection instruments, study sample and the case studies involved in the study. Chapter Four presented the findings of the study from data collected through documentary reviews and interviews. Chapter Five offered a broad interpretation of the findings of the study while Chapter 6 provides a summary of the study findings, conclusions and recommendations as informed by the findings of the study. A proposed framework for the authentication of digital records in a government accounting system to support audit processes in the public sector of Botswana was presented.

This study has shown that a supportive legislative framework is a necessity in order to facilitate digital accounting records that can support the audit process lest auditors throw out such records if their authentication is suspect. Although the principal archival legislation was found wanting to guide the creation and maintenance of authentic records created through business systems (i.e. GABS), other legislation such as the Electronic Records (Evidence) Act, Cybercrime and Computer Crimes Related Act and the Electronic Telecommunications Act have adequate provisions to guide the maintenance of records authenticity.

Secondly, procedures exist for the authenticating of digital records in GABS. ICT professionals use both technical and social indicators of assessing records authenticity while auditors use CAATs to verify the authenticity of accounting records to be used as audit evidence in the audit process. It is also clear that records management professionals have limitations, as they could not deal with digital records management issues, including those related to the authenticity of records in business systems. This was confirmed by the findings related to the skills and competencies required for authenticating digital accounting records in GABS. It emerged that they lacked computing skills needed to navigate the digital world. Auditors were equipped with the necessary skills and competencies, but still felt continuous training and retraining was a necessity in order to keep pace with technological advancements. As for ICT professionals, they are well equipped in terms of skills and competencies.

Findings on the objective dealing with the management of digital accounting records created through GABS showed that the system created truly digital records when assessed through the archival diplomatics lens. However, the retention and disposal of such records are poorly handled. Firstly, since the system was implemented in 2004, accounting records still reside in the system as if it is an archiving system. Secondly, although records retention and disposal schedules for accounting and finance records do exist, these have not been configured into the system to facilitate records retention and disposal. It was encouraging to discover that there are some management efforts to ensure continued availability of records in the system for as long as needed. It is concluded that due to failure to establish guidelines and checklists for auditors to authenticate digital records, they will continue to rely on IT and system application controls so it is recommended that the Auditor General develop a checklist for the authentication of digital records.

References

Abiola, JO. 2013. The impact of information and communication technology on internal control's prevention and detection of fraud. Available at: https://www.dora.dmu.ac.uk/bitstream/handle/2086/9496/james%20abiola%20thesis.pdf (Accessed 20 September 2017).

Abiola, JO. 2014. The impact of information and communication technology on internal auditors' independence: A PEST Analysis of Nigeria. *Journal of Scientific Research & Reports* 3(13):1732-1752.

Abioye, A. 2007. Fifty years of archives administration in Nigeria: lessons for the future. *Records Management Journal* 17(1):52-62.

Abuzawayda, YI, Mohd, ZY & Mohd, AA. 2013. Electronic records management in institutions of higher learning in Libya: adoption of DIRKS Model. *Journal of Theoretical and Applied Information Technology* 53(3):346-352.

ACCA. 2011. Specific aspects of auditing in a computer-based environment. Available at: https://www.coursehero.com/file/17883767/9-sa-jan11-CAATs/ (Accessed 23 November 2018.

Adams J, Khan, HTA, Raeside, R & White, D. 2007. *Research methods for graduate business and social science students*. London: Response Books.

Adhabi, E & Anozie, CB. 2017. Literature review for the type of interview in qualitative research. *International Journal of Education* 9(3):86-97.

Adu, KF. 2015. *Framework for digital preservation of electronic government in Ghana*. Doctor of Philosophy and Literature, University of South Africa, Pretoria.

Adu, KF & Ngulube, P. 2017. Key threats and challenges to the preservation of digital records of public institutions in Ghana. Information, Communication & Society 20(8):1127-1145.

Ahmed, JU. 2010. Documentary research method: new dimensions. *Indus Journal of Management & Social Sciences* 4(1):1-14.

Ahmed, A & Sil, R. 2012. When multi-method research subverts methodological pluralism – or, why we still need single-method research. *Perspectives on Politics* 10(4):935-953.

Ahmi, A & Kent. S. 2013. The utilisation of generalized audit software (GAS) by external auditors. *Managerial Auditing Journal* 28(2):88-113.

Aina, LO. 2002. Introduction to research, in Aina, LO. 2002. (Ed.) *Research in information sciences: an African perspective.* Ibadan: Stirling – Horden Publishers.

Akinyemi, B, Okoye, AE & Izedonmi, PF. 2015. History and development of accounting in perspective. *International Journal of Sustainable Development Research* 1(2):14-20.

Akotia, P. 1996. The management of public sector financial records: the implications for good government. Available at: http://www.msu.ac.zw/elearning/material/1174370018Pino%20Akotia%201996%20on%20governance.pdf (Accessed 20 August 2016).

Alhojailan, MI. 2012. Thematic analysis: a critical review of its process and evaluation. *West East Journal of Social Sciences* 1(1):39-47.

Alshengeeti, H. 2014. Interviewing as a data collection method: a critical analysis. *English Linguistics Research* 3(1):39-45.

Amankwaa, L. 2016. Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity* 23(3):121-127.

Amatya, S. 2016. Practice of ICT for effective implementation of internal control system and internal audit in the context of Nepalese NGOs. *International Journal for Innovation Research in Multidisciplinary Field* 2(7):82-92.

Ambashe, MA & Alrawi, HA. 2013. The development of accounting through the history. *International Journal of Advances in Management and Economics* 2(2):95-100.

Ambira, CM. 2016. A framework for management of electronic records in support of e-government in Kenya. PhD Thesis, University of South Africa. Pretoria.

American Anthropological Association. 2009. Code of Ethics of the American Anthropological Association. Available at: http://www.aaanet.org/issues/policy-advocacy/upload/AAA-Ethics-Code-2009.pdf Accessed 23 February 2015.

Anderson, K. 2013. Recordkeeping definitions in legislation: a conceptual step towards smoothing business interaction in the digitally networked world? Available at: https://www.archivists.org.au/documents/item/461 (Accessed 20 July 2016).

Arora, J. 2006. Digital preservation: an overview. Available at: http://ir.inflibnet.ac.in:8080/ir/bitstream/1944/1466/1/8.pdf (Accessed 26 March 2018).

Arumugam, V, Jiju, A & Douglas, A. 2012. Observation: a lean tool for improving the effectiveness of Lean Six Sigma. *The TQM Journal* 24(3):275 – 287.

Asogwa, BE 2012. The challenge of managing electronic records in developing countries: implications for records managers in sub-Saharan Africa. *Records Management Journal* 22(3):198-211.

Asproth. V. 2005. Information technology challenges long term preservation of electronic information. Available at: http://www.diva-portal.org/smash/get/diva2:29271/fulltext01.pdf (Accessed 19 December 2017).

Atherton, J. 1985. From lifecycle to continuum: some thoughts on the records management archives relationship. *Archivaria* 21:43-51.

Auditor General of South Africa. 2014. 2013-14 Consolidated general report on local Government audit outcomes. Available at: http://intranet/AGSADocuments/AuditReports/Documents/2013-14%20MFMA/MFMA%20201314%20Consolidated%20GR%20Part%207%20Section%204%20Status%20of%20performance%20management.pdf (Accessed 11 July 2017).

Austen, LA, Eilifsen, A & Messier, WF. 2003. Auditor detected misstatements and the effect of Information Technology. Available at: https://core.ac.uk/download/pdf/52069378.pdf (Accessed 3 December 2018).

Australian Accounting Research Foundation. 2002. *Electronic Commerce - Effect on the Audit of a Financial Report*. Melbourne: Australian Accounting Research Foundation.

Australia National Audit Office. 2012. Records management in the Australian public service. Available at: https://www.anao.gov.au/sites/g/files/net1621/f/201112%20Audit%20Report%20No%2053.pdf (Accessed 29 July 2016).

Australian Capital Territory. 2008. Guideline for records management number 8 – business continuity and records management. Available at: https://www.territoryrecords.act.gov.au/__data/assets/pdf_file/0006/472704/Guideline-No-8-Business-Continuity-August-2008.pdf (Accessed 11 March 2018).

Babbie, E. 2007. *The practice of social research*. United States: Thomson Wadsworth.

Babbie, E. 2011. *The basics of social research*. 6th edition. Wadsworth: Cengage.

Babbie, E & Mouton, J. 2001. *The practice of social research*. Cape Town: Oxford University Press.

Baillie, L. 2015. Promoting and evaluating scientific rigour in qualitative research. *Nursing Standard* 29(46):36-42

Bantin, PC. 2008. *Understanding data and information systems for recordkeeping*. London, New York: Neal-Schuman Publishers.

Barreiro, PL & Albandoz, JP. 2001. Population and sample: sampling techniques. Available at: http://optimierung.mathematik.unikl.de/mamaeusch/veroeffentlichungen/ver_texte/sampling_en.pdf (Accessed 3 June 2017).

Barrister, MS. 2006. Proof of the authenticity of a document in electronic format introduced as evidence. Available at: http://www.mnhs.org/preserve/records/legislativerecords/docs_pdfs/Proof_of_authenticity_of_a_document.pdf (Accessed 3 April 2016).

Beagrie, N & Greenstein, D. 1998. *A strategic policy framework for creating and preserving digital collections*. London: Library Information Technology Centre.

Bearman, D. 1993. Record-keeping systems. *Archivaria* 36 (Autumn):16-36.

Bearman, D. 2007. Electronic evidence: strategies for managing records in contemporary organisations. *Archives and Museums Informatics*, Pittsburgh, Pa.

Bearman, D & Sochats, 2004. Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project. Available at: http://www.archimuse.com/papers/nhprc/BACartic.html (Accessed 23 November 2018).

Becker Professional Education. 2012. The 10 GAAS standards and the "old" auditor is reporting model. Available at: https://studylib.net/doc/8110226/the-10-gaas-standards-and-the---becker-professional-educa... (Accessed 18 November 2018).

Benbasat, I, Goldstein, DK & Mead, M. 1987. The case research strategy in studies of information systems. *MIS Quarterly*/September: 369-386.

Benoliel, JQ. 1996. Grounded theory and nursing knowledge. *Qualitative Health Research* 6:406-428.

Berg, BL. 2007. *Qualitative research methods for the social sciences*. London: Pearson.

Berman, J. 2013. Utility of a conceptual framework within doctoral study: a researcher's reflections. *Issues in Educational Research* 23(1):1-18.

Bernard, HR. 2000. *Social research methods: qualitative and quantitative approaches*. Thousand Oaks, CA: Sage Publications.

Bernard, HR. 2013. *Social research methods: qualitative and quantitative approaches*, 2nd edition. London: SAGE Publications Ltd.

Bhana, P. 2008. *The contribution of proper record-keeping towards auditing and risk mitigation: Auditor-General of South Africa's perspective*. Paper presented at the 3rd Annual General Meeting of the South African Records Management Forum, Midrand (South Africa), 10 - 11 November. Available at: http://www.khunkhwane.co.za/uploads/The%20Contribution%20of%20Proper%20Records%20Keeping%20towards%20auditing%20and%20risk%20mitigation%20%20Auditor %20General%20Perspective.pdf (Accessed 20 April 2017).

Bhattacherjee, A. 2012. *Social science research: principles, methods and practices*. Zurich: Creative Commons Attribution. Available at: http://www.saylor.org/site/wp-content/uploads/2012/01/ POLSC251BHATTACHERJEETEXTBOOK.pdf (Accessed 7 February 2016).

Bhebhe, S. 2015. Contemporary diplomatics of the civil and deceased estate case files found at the national archives of Zimbabwe. *Records Management Journal* 25(1):107-120.

Bhebhe, S, Masuku, M & Ngulube, P. 2013. Infrastructural challenges on archives and recordkeeping at the National Archives of Zimbabwe. *Journal of the South African Society of Archivists* 46:47-62.

Blum, K. 2006. Teaching students how to write a chapter four and five of a dissertation. Available at: http://community.csusm.edu/mod/resource/view.php?id=371 (Accessed 21 November 2017).

Blythe, SE. 2007. Hungary's Electronic Signature Act: enhancing economic development with secure e-commerce transactions. *Information and Communications Technology Law* 16(1):47-71.

BOCRA. 2015. Consultation paper on the Electronic Communications and Transactions Regulations. Available at: http://www.bocra.org.bw/sites/default/files/documents/ECTR%20Consultation%20Document.pdf (Accessed 30 July 2017).

Botswana Gazette. 2014. *Government records in a big mess*, 12 June.

Botswana Telecommunications Corporation. 2017. *Phone Book 2017*. Gaborone: Botswana Telecommunications Corporation Limited.

Boudrez, F. 2005. Digital signatures and electronic records. Available at: http://www.expertisecentrumdavid.be/docs/digitalsignatures.pdf (Accessed 16 November 2018).

Bowen, GA. 2009. Document analysis as a qualitative research method. *Qualitative Research Journal* 9(2):27-40.

Boyce, C & Neale, P. 2006. *Conducting in-depth interviews: a guide for designing and conducting in-depth interviews for evaluation input*. Available at: http://www2.pathfinder.org/site/DocServer/m_e_tool_series_indepth_interviews.pdf (Accessed 23 November 2018).

Bradburn, N, Sudman, S & Wansink, B. 2004. *The definitive guide to questionnaire design – for market research, political polls, and social and health questionnaires*, 1st edition. San Francisco: Jossey-Bass.

Bradley, R. 2005. Digital authenticity and integrity: digital cultural heritage documents as research resources. *Portal: Libraries and the Academy* 5(2):165-175.

Brand, S. 1999. Escaping the digital Dark Age. Available at: http://www.rense.com/general38/escap.htm (Accessed 17 January 2017).

Braun, V & Clarke, V. 2006. Using thematic analysis in psychology. http://eprints.uwe.ac.uk/11735/2/thematic_analysis_revised...(Accessed 21 November 2017).

Braun, V & Clarke, V. 2012. Thematic analysis, in Cooper, H (ed.), *The handbook of research methods in psychology*. Washington, DC: American Psychological Association.

Brewerton, P & Millward, L. 2001. *Organisational research methods*, London: Sage Publications Ltd.

British Broadcasting Corporation. 2010. Records management standard for the BBC. Available at: http://www.bbc.co.uk/guidelines/dq/pdf/media/records_management_standards_v1.3.pdf (Accessed 3 March 2018).

Bryman, A. 2004. *Social research methods,* Oxford: Oxford University Press.

Bryman, A. 2012. *Social research methods*, New York: Oxford University Press.

Burnard, P, Gill, P, Stewart, K, Treasure, E & Chadwick, B. 2008. Analysing and presenting qualitative data. *British Dental Journal* 204(8):429-432.

Burns, R. 2000. Introduction to Research Methods. 4th edition. London, Sage

Bushey, J. 2016. The archival trustworthiness of digital photographs in social media platforms. PhD Thesis, University of British Columbia, Vancouver.

Bwalya, KJ. 2011. *E-government adoption and synthesis in Zambia: context, issues and challenges*. PhD Thesis, University of Johannesburg, Pretoria.

Carroll, M. 2006. *An information systems auditor's profile*, MSc Dissertation, University of South Africa, Pretoria.

Caruth, GD. 2013. Demystifying mixed methods research design: a review of the literature. *Mevlana International Journal of Education* (MIJE) 3(2): 112-122.

Case, DO & Given, LM. 2016. *Looking for information: a survey of research on information seeking, needs, and behaviour*. 4th edition. Bingley, UK: Emerald Group Publishing.

Center for Drug Evaluation and Research. 2017. Electronic and digital signatures for records management. Available at:

https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ManualofPoliciesProcedures/UCM576742.pdf (Accessed 5 May 2018).

Center for Technology in Government. 2003. Digital signatures and authentication. Available at: https://www.ctg.albany.edu/publications/reports/key_concepts?chapter=2&PrintVersion=2 (Accessed 7 May 2018).

Chadha. RK. 2009. Digital preservation: strategies for Indian libraries. Available at: http://inflibnet.ac.in/caliber2009/CaliberPDF/1.pdf (Accessed 21 March 2018).

Charles Darwin University. 2014. *Records management – capturing university records procedures*. Available at: https://www.cdu.edu.au/governance/doclibrary/pro-061.pdf (Accessed 5 October 2017).

Chartered Accountants Australia and New Zealand.2016. Guidance on the auditor competency standard for registration as a registered company auditor. Available at: file:///C:/Users/omosweu/Downloads/Auditor%20registration%20competency%20guide.pdf (Accessed 22 May 2018).

Chêne, M. 2009. The Implementation of integrated financial information management systems (IFMS). Available at: http://www.u4.no/publications/the-implementation-of-integrated-financialmanagement-systems-ifmis/ (Accessed 17 January 2017).

Clarke, V & Braun, V. 2013. Teaching thematic analysis: overcoming challenges and developing strategies for effective learning. *The Psychologist* 26(2):120-123.

Cloonan, MV & Sanett, S. 2002. Preservation strategies for electronic records: where we are now—obliquity and squint? *The American Archivist* 65 (April/Summer):70 -106.

Cohen, L, Manion, L & Morrison, K. 2007. *Research methods in education*. 6th edition. New York: Routledge.

Coleman, K. 2008. The key to data security: separation of duties. Available at: https://www.computerworld.com/article/2532680/technology-law-regulation/the-key-to-data-security--separation-of-duties.html (Accessed 10 May 2018).

Committee on Electronic Records. 1997. *Guide for managing electronic records from an archival perspective*. Paris, France: International Council on Archives.

Connelly, LM. 2016. Trustworthiness in qualitative research. *Medsurg Nursing* 25(6):435-436.

Cook, M. 1986. *The management of information from archives*. Aldershot, Hants, England, Brookfield, Vt., U.S.A: Gower.

Coolican, H. 1999. *Aspects of psychology: research methods and statistics*. London: Hodder & Stoughton.

CPA Australia. 2014. A guide to understanding auditing and assurance. Available at: https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/auditing-assurance/guide-understanding-audit-assurance.pdf?la=en (Accessed 29 November 2018).

Council of Europe. 2001a. Convention on cybercrime. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (Accessed 24 April 2018).

Council of Europe. 2001b. *Explanatory report to the convention on cybercrime*. Available at: https://rm.coe.int/16800cce5b (Accessed 24 April 2018).

Cox, RJ. 1997. Electronic systems and records management in the information age: an introduction. Available at: http://onlinelibrary.wiley.com/doi/10.1002/bult.59/full (Accessed 12 December 2016).

Cox, R. 1997. More than diplomatic: functional requirements for evidence in recordkeeping. *Records Management Journal* 7(1):31-57.

CRC Press. 2001. Records management guidance for implementing electronic signature technologies, *EDPACS* (28)9:1-11.

Creswell, JW. 2003. *Research design: a qualitative, quantitative and mixed method approaches*. Californian: Sage Publications Inc.

Creswell, JW. 2006. *Understanding mixed method research*. California: SAGE Publications.

Creswell, JW. 2007. *Qualitative inquiry and research design: Choosing among five approaches*. Thousand Oaks CA: Sage.

Creswell, JW. 2009. *Research design.* Thousand Oaks, CA: Sage.

Creswell, JW. 2014. *Research design: qualitative, quantitative, and mixed methods approaches*. Los Angeles: Sage Publications.

Crotty, M. 1998. *The foundations of social research: meaning and perspective in the research process*. Thousand Oaks, CA: Sage.

Cumming, K & Findlay, C. 2010. Digital records keeping; are we at a tipping point? *Records Management Journal* 20(3):265-278.

Curtis, MB, Jenkins, JG, Bedard, JC & Deis, DR. 2009. Auditors' training and proficiency in information systems: a research synthesis. *Journal of Information Systems* 23(1):79-96.

Dahiya, Y & Sangwan, S. 2014. Computer and network forensics: imaging digital evidence. *International Journal of Emerging Research in Management &Technology* 3(5):105-111.

Danish National Archives. 2013. *Strategy for archiving digital records at the Danish National Archives.* Available at: https://www.sa.dk/wp-content/uploads/2014/12/Strategy-for-archiving-digital-records-2013.pdf (Accessed 7 May 2018).

David, R. 2017. Contribution of records management to audit opinions and accountability in government. *South African Journal of Information Management* 19(1):1-14.

Day, M. 1999. Issues and approaches to preservation metadata. Available at: http://opus.bath.ac.uk/23708/1/paper.pdf (Accessed 20 May 2017).

Day, M. 2001. Metadata for digital preservation: a review of recent developments. Available at: http://opus.bath.ac.uk/23596/1/springer-version.pdf (Accessed 22 19 May 2017).

De Benetti, T. 2009. The role of theory in research. Available at: https://www.researchgate.net/publication/201834276 (Accessed 25 April 2018).

Debreceny, R, Lee, S, Neo, W & Toh, JS. 2005. Employing generalized audit software in the financial services sector: challenges and opportunities. *Managerial Auditing Journal* 20(6):605-619.

De Jager, H. 2008. Editorial: auditing and credibility. *Auditing SA Summer edition*: 3-4.

Dennis, A, Wixom, BH & Roth, RM. 2012. *System analysis and design*. Hoboken: John Wiley & Sons.

Denzin, NK. 2008. The new paradigm dialogs and qualitative inquiry. Available at: http://in.bgu.ac.il/icqm/DocLib/Pages/2008/Norman%20K.%20Denzin.pdf (Accessed 26 May 2017).

Denzin, NK & Lincoln, YS. 2000. *Handbook of qualitative research*. 2nd edition. London: Sage Publications.

Denzin, NK & Lincoln, YS. 2005. Introduction: the discipline and practice of qualitative research, in Denzin, N & Lincoln Y. (eds.), *The SAGE handbook of qualitative research.* Thousand Oaks, CA: Sage.

Denscombe, M. 2007. *The good research guide for small-scale social research projects. Berkshire*, Open University Press.

Department of Health and Human Sciences 2009. Data collection methods for evaluation: document review. Available at: https://www.cdc.gov/healthyyouth/evaluation/pdf/brief18.pdf (Accessed 23 June 2017).

De Vos, AS, Strydom, H, Fouche, CB & Delport, CSL. 2011. *Research at grass roots: for the social sciences and human service professions*. Pretoria: Van Schaik.

Dezan Shira and Associates. 2013. An introduction to audit in India. Available at: https://keitercpa.com/wp-content/uploads/2013/06/An-Introduction-to-Audit-in-India.pdf (Accessed 25 June 2018).

Dilevko, J. 2007. Reading literature and literature reviews. *Library & Information Science Research* 29:451-454.

Director, CW. 2005. Diplomatic attitudes: from Mabillion to metadata. *Journal of Society of Archivists* 26(1):1-24.

Dörnyei, Z. 2007. *Research methods in applied linguistics; quantitative, qualitative and mixed methodologies*. Oxford: Oxford University Press.

Duff, W. 1996. Ensuring the preservation of reliable evidence: a research project funded by the NHPRC. *Archivaria* 42:28-45.

Dumortier, J & Eynde, SVD. 2002. Electronic signatures and trusted archival services. Available at:

http://www.edavid.be/davidproject/teksten/DAVIDbijdragen/Tas.pdf (Accessed 13 November 2018).

Duranti, L. 1989. *Diplomatics: new uses for an old science*. London: The Scarecrow Press.

Duranti, L. 1994. ‘The concept of appraisal and archival theory’. *American Archivist* 57:328-344.

Duranti, L. 1995. Reliability and authenticity: the concepts and their implications. *Archivaria* 39:5-10.

Duranti, L. 1997. The archival bond. *Archives and Museum Informatics* 11:213-218.

Duranti, L. 2001. Concepts, principles, and methods for the management of electronic records. *The Information Society* 17:271-279.

Duranti, L. 2005. Authenticity and authentication in the law. Available at: http://www.interpares.org/display_file.cfm?doc=ip2(policy)authenticity-authentication_law.pdf (Accessed 16 March 2017).

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

Duranti, L. 2010. Concepts and principles for the management of electronic records, or records management theory is archival diplomatics. *Records Management Journal* 20(1):78-95.

Duranti, L. 2014. Involuntary secondary permanence: do many copies replace the one original? Available at: https://interparestrust.org/assets/public/dissemination/Duranti_2014_YaleLibraries.pdf (Accessed 4 January 2017).

Duranti, L & Blanchette, JF. 2004. The authenticity of electronic records: the InterPARES approach. Available at: https://pages.gseis.ucla.edu/faculty/blanchette/papers/ist2.pdf (Accessed 12 May 2018).

Duranti, L, Eastwood, T & MacNeil, H. 2002. *Preservation of the integrity of electronic records*. Dordrecht: Kluwer Academic Publishers.

Duranti, L & Jansen, A. 2011. Authenticity of digital records: an archival diplomatics framework for digital forensics. Paper presented at the September ECIME, 2011 (Como, Italy) Conference. Available at: https://www.researchgate.net/publication/290042000_Authenticity_of_digital_records_An_archival_diplomatics_framework_for_digital_forensics (Accessed 21 April 2018).

Duranti, L & MacNeil, H. 1996. The protection of the integrity of electronic records: an overview of the UBC-MAS Research Project. *Archivaria* 42:46-67.

Duranti, L & Rogers, C. 2012. Trust in digital records: an increasingly cloudy legal area. *Computer Law and Security Review* 28:522-531.

Duranti, L & Thibodeau, K. 2006. The concept of record in interactive, experiential and dynamic environments: the view of InterPARES. *Archival Science* 6(1):13-68.

Duranti, L, Rogers, C & Sheppard, A. 2010. Electronic records and the law of evidence in Canada: the Uniform Electronic Evidence Act twelve years later. *Archivaria 70 (Fall)*:95-124.

Duranti, L & Takashi, K. 2013. Trusting digital records: the major findings of the InterPARES Project. Available at: https://repository.kulib.kyoto-u.ac.jp/dspace/bitstream/2433/173414/1/kua11_15.pdf (Accessed 26 July 2017).

Eastwood, T. 1994. What is archival theory and why is it important? *Archivaria 37*: 122-130.

Eastwood, T. 2006. Building archival knowledge and skills in the digital age. *Archival Science* 6: 163-170.

Eisenhardt, KM. 1989. Building theories from case study research. *The Academy of Management Review* 14(4):532-550.

Eisenhardt, KM. & Graebner, ME. 2007. Theory building from cases: opportunities and challenges. *Academy of Management Journal* 50(1):25-32.

Elder, RJ, Beasley, MS & Arens, AA. 2010. *Auditing and assurance services: an integrated approach: global edition*. Prentice-Hall: Englewood Cliffs.

Elefterie, L & Badea, G. 2016. The impact of information technology on the audit process. Economics. *Management and Financial Markets* 11(1):303-309.

Elliot, MH. 2007. Record integrity and authentication for electronic R&D. Available at: http://www.atriumresearch.com/library/Record_Authentication_and_Integrity.pdf (Accessed 22 May 2018).

Ellison, N. 2010. *Research methods. a practical guide for the social sciences*. Sydney: Pearson.

Ernest & Young 2010. A risk-based approach to segregation of duties. Available at: http://www.ey.com/Publication/vwLUAssets/EY_Segregation_of_duties/$FILE/EY_Segregation_of_duties.pdf (Accessed 10 May 2018).

Erlandsson, A. 1997. Electronic records management: a literature review. Available at: http://www.na.ae/en/Images/ICA_Study-10-Electronic-records-management-literature-review_EN.pdf (Accessed 3 April 2017).

Essner, N & Unander-Scharin, E. 2013. Analytical procedures - a practice based approach. Available at: http://www.diva-portal.org/smash/get/diva2:630208/FULLTEXT02 (Accessed 9 January 2017).

European Commission. 2008. Model requirements for the management of electronic records. Available at: http://www.interpares.org/display_file.cfm?doc=ip2_dissemination_rep_moreq2_2008.pdf (Accessed 17 May 2018).

European Commission Delegation Botswana. 2009. Public expenditure and financial accountability: public financial management performance assessment report. Available at: https://ec.europa.eu/europeaid/sites/devco/files/report-pefa-assessment-botswana-200902_en.pdf (Accessed 16 November 2018).

European Commission. 2015. New EU regulation for electronic signatures. Available at: https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/ (Accessed 29 November 2018).

European Universities Association. 2010. Salzburg II Recommendations - European universities' achievements since 2005 in implementing the Salzburg Principles. Brussels: EUA. Available at:

http://www.eua.be/Libraries/publications-homepage-list/Salzburg_II_Recommendations (Accessed 16 May 2016).

Evans, D & Yen. DC. 2005. E-government: an analysis for implementation: framework for understanding cultural and social impact. *Government Information Quarterly*: 29-41.

Fang, Z. 2002. E-government in digital era: concept, practice, and development. *International Journal of the Computer, the Internet and Management* 10(2):1-22.

Flick, U. 2013. The Sage handbook of qualitative data analysis. Available at: http://www.ewi-psy.fu-berlin.de/einrichtungen/arbeitsbereiche/qualitative_sozial-_bildungsforschung/Medien/58869_Flick__The_SAGE_HB_of_Qualitative_Data_Analysis_Chapter1_mapping-the-field.pdf (Accessed 18 December 2017).

Force, DC. 2013. Pursuing the "usual and ordinary course of business": an exploratory study of the role of recordkeeping standards in the use of records as evidence in Canada. PhD Thesis, University of British Columbia, Vancouver.

Fox, N. 1998. How to use observations in a research project? Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.529.5902&rep=rep1&type=pdf (Accessed 25 July 2017).

Fox, N. 2009. Using interviews in a research project. Available at: https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/15_Using-Interviews-2009.pdf (Accessed 10 June 2017).

Franks, P & Kunde, N. 2006. Why metadata matters. Available at:
http://www.arma.org/bookstore/files/Franks-Kunde1.pdf (Accessed 1 July 2016).

Gall, MD, Borg, WR & Gall, JP. 1996. *Education research: An introduction.* White Plains, NY: Longman.

Ganetsang, G. 2015. Government aligns legislature to technological developments. *Sunday Standard*, 22 March 2015.

Garderen, PV, Jordan, P, Hooten, T, Mumma & McLellan, E. n.d. The Archivematica project meeting digital continuity's technical challenges. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/mow/VC_Van_Garderen_et_al_26_Workshop1.pdf (Accessed 21 November 2018).

Gasson, S. 2004. Rigor in grounded theory research: An interpretive perspective on generating theory from qualitative field studies, in Whitman ME & Woszczynski AB (eds.), *The handbook of information systems research*, Hershey, PA: Idea Group.

Gear, J. 2013. Is the EU "Going Too Far"? Examining the divide between the legislator within the EU and members of the financial market. Available at: https://skemman.is/bitstream/1946/14451/1/Is%20the%20EU%20going%20too%20far.pdf (Accessed 18 May 2018).

Gentles, SJ, Charles, C, Ploeg, J & McKibbon, KA. 2015. Sampling in qualitative research: insights from an overview of the methods literature. *The Qualitative Report* 20(11): 1772-1789.

Gereda, SL. 2003. The Electronic Communications and Transactions Act. Available at: http://thornton.co.za/resources/telelaw12.pdf (Accessed 21 April 2018).

Gibson, A. 2001. Overview of the diplomatic analysis of electronic records within the Canadian automated patent system (TechSource), in Sarno, L (ed). 2001. Preserving electronic records: preliminary research findings. Available at: http://www.interpares.org/documents/interpares_symposium_2001.pdf (Accessed 6 January 2017).

Gilliland-Swetland, AJ. 2000. Setting the stage. Available at: http://marciazeng.slis.kent.edu/metadata/Gilland.pdf (Accessed 25 July 2016).

Goh, E. 2014. Clear skies or cloudy forecast? Legal challenges in the management and acquisition of audiovisual materials in the cloud. *Records Management Journal* 24(1):56-73.

Goh, EMY. 2016. Archival law from the trenches: the impact of archival legislation on records management in Commonwealth countries. PhD Thesis, University of British Columbia, Vancouver. Available at: https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0300019 (Accessed 26 April 2018).

Goh, E & Duranti, L. 2012. Archival legislation for engendering trust in an increasingly networked digital environment. Available at:

http://ica2012.ica.org/files/pdf/Full%20papers%20upload/ica12Final00287.pdf (Accessed 20 April 2018).

Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report* 8(4):597-607.

Goldkuhl, G. 2012. Pragmatism vs interpretivism in qualitative information systems research, 2012. *European Journal of Information Systems* 21(2):135-146.

Gorard, S & Taylor, C. 2004. *Combining methods in educational and social research*. London: Open University Press.

Government of Botswana. 1966a. *Constitution of Botswana, Cap 0000*, Gaborone: Government Printer.

Government of Botswana. 1966b. *Foreign Documents Evidence, Cap 14:03*. Gaborone: Government Printer.

Government of Botswana. 1970. *Authentication of documents, Cap 14:02*. Gaborone: Government Printer.

Government of Botswana. 1978. *National Archives and Records Services Act*, Cap 59:04. Gaborone: Government Printer.

Government of Botswana. 1993. *Financial Instructions and Procedures*, Gaborone: Government Printer.

Government of Botswana. 2004. *Criminal Procedure and Evidence Act, Cap 08:02*. Gaborone: Government Printer.

Government of Botswana. 2007. *Cybercrimes and Computer Related Crimes Act, Cap 08:06*. Gaborone: Government Printer.

Government of Botswana. 2011a. *Botswana's National E Government Strategy 2011 – 2016*, Gaborone: Government Printer.

Government of Botswana. 2011b. *Public Finance Management Act*, Gaborone: Government Printer.

Government of Botswana. 2012. *Public Audit Act*, Cap 54:02. Gaborone: Government Printer.

Government of Botswana. 2014a. *Electronic records (Evidence) Act*, Gaborone: Government Printer.

Government of Botswana. 2014b. *Electronic Communications and Transactions Act*, Gaborone: Government Printer.

Government of Botswana. 2017a. Internal Audit Department. Available at: http://www.gov.bw/en/Ministries--Authorities/Ministries/Ministry-of-Finance-and-Development-Planning/Departments/Internal-Audit/ (Accessed 29 July 2017).

Government of Botswana. 2017b. *Cybercrimes and Computer Related Crimes Bill*. Gaborone: Government Printer.

Government of Canada. 2004. Library and Archives Act. Available at: http://laws-lois.justice.gc.ca/eng/acts/L-7.7/page-1.html (Accessed 3 August 2016).

Government of Hong Kong. 2011. Good records management practices. Available at: http://www.grs.gov.hk/ws/english/engimages/grmp_e.pdf (Accessed 13 December 2017).

Government of Mauritius. 2000. The Electronic Transactions Act. Available at: http://www.mcci.org/media/36445/electronic-transaction-act-2000.pdf (Accessed 27 September 2016).

Government Records Service 2013. A handbook on preservation of electronic records. Available at: http://www.grs.gov.hk/pdf/A_Handbook_on_Preservation_of_Electronic_Records_(July_2013)(Eng_only).pdf (Accessed 25 February 2018).

Government of South Africa. 1996. National Archives and Record Service of South Africa Act. Available at: http://www.kznworks.gov.za/publications/policy/National_Archives_Act_and_Regulations.pdf (Accessed 21 May 2016).

Government of South Africa. 2002a. Electronic Telecommunications Act. Available at: http://www.up.ac.za/media/shared/409/ZP_Files/25-of-2002-electronic-communications-and-transactions-act_31-ma.zp44223.pdf (Accessed 26 September 2016).

Government of South Africa. 2002b. Regulation of Interception of Communication and Provision of Communication-related Information Act. Available at: http://www.justice.gov.za/legislation/acts/2002-070.pdf (Accessed 24 July 2017).

Government of South Australia. 2007. Records management disaster planning. Available: https://government.archives.sa.gov.au/sites/default/files/20120125%20Records%20Management%20Disaster%20Planning%20%20Final%20V1.2_Copy.pdf (Accessed 8 May 2018).

Government of South Australia. 2014. Implementing a records disposal programme. Available at: https://government.archives.sa.gov.au/sites/default/files/20140410%20Records%20Disposal%20Program%20Planning%20Final%20V1_Copy.pdf (Accessed 10 October 2017).

Grant, C & Osanloo, A. 2014. Understanding, selecting, and integrating a theoretical framework in dissertation research: creating the blueprint for your "house". *Administrative Issues Journal: Connecting Education, Practice and Research* 4(2):12-26.

Gränström, C, Hornfeldt, T, Peterson, G, Mariana, MPR, Schäfer, U & Zwicker, J. 2002. Authenticity of electronic records: a report prepared for UNESCO. Available: https://www.ica.org/sites/default/files/ICA_Study-13-1-Authenticity-of-electronic-records-ICA-Report-to-UNESCO_EN.pdf (Accessed 21 April 2018).

Gray, DE. 2009. *Doing research in the real world.* London: Sage Publications.

Green, H. 2014. Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher* 21(6):34-38.

Gubrium, JF & Holstein, JA. 2002. *Handbook of interview research: context and methods*, Thousand Oaks, CA: Sage.

Guetzkow, J, Lamont, M & Mallard, G. 2004. What is originality in the humanities and the social sciences? *American Sociological Review* 69(2):190-212.

Gustavson, M. 2013. *Auditing good government in Africa: public sector reform, professional norms and the development discourse*. New York: Palgrave Macmillan.

Gustavson, M. 2015. Does good auditing generate quality of government? Available at: https://qog.pol.gu.se/digitalAssets/1538/1538160_2015_15_gustavson.pdf (Accessed 17 November 2018).

Hamooya, C, Mulauzi, F & Njobvu, B. 2011. Archival legislation and the management of public sector records in Zambia: a critical review. *Journal of the South African Society of Archivists* (44):116-123.

Hancock, B, Ockleford, E & Windridge, K. 2009. An introduction to qualitative research. Available at: https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/5_Introduction-to-qualitative-research-2009.pdf (Accessed 12 June 2017).

Hargreaves, C & Forasacco, E. 2015. Literature review. Available at: https://www.imperial.ac.uk/media/imperial-college/study/graduate-school/public/helpsheets/Reviewing-the-Literature-Doctoral-2015.pdf (Accessed 2 March 2017).

Harrison, RL. & Reilly, TM. 2011. Mixed methods designs in marketing research. *Qualitative Market Research: An International Journal 14* (1): 7-26.

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 (Accessed 26 September 2016).

Hendricks. CJ. 2012. Integrated financial management information systems: guidelines for effective implementation by the public sector of South Africa. *South African Journal of Information Management* 14(1):1-9.

Hernon, P & Schwartz, C. 2009a. Procedures: research design. *Library and Information Science Research Editorial* 31:1-2.

Hernon, P & Schwartz, C. 2009b. Reliability and validity. *Library and Information Science Research* 31:73-74.

Herrera, H. 2011. *Language and archival vocabulary: [something more than a dictionary] Basic data*. Seville: General Directorate of Books, Archives and Libraries.

Hoke, GEJ. 2012. *Future watch*: strategies for long-term preservation of electronic records. Available at: http://content.arma.org/IMM/Libraries/May-June_2012/IMM_0512_Full_Issue.sflb.ashx (Accessed 3 March 2018).

Holland, J & Campbell, J. 2005. *Methods in development research*: *combining qualitative and quantitative Approaches*. London: ITDG.

Holmes, M & Bloxham, M. 2007. An observational method for time use research: Advantages, disadvantages and lessons learned from the Middletown Media Studies. Presented at the 2007 Conference of the International Association of Time Use Researchers, Washington. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.489.5992&rep=rep1&type=pdf (Accessed 25 July 2017).

Hunter, GS. 2000. *Preserving digital information: a how-to-do-it manual*. New York: Neal-Schuman Publishers.

Hurley, C. 2005. Recordkeeping and accountability. In McKemmish, S, Piggott, M, Reed, B, & Upward, F. (Eds) *Archives: Recordkeeping in society*, (pp. 223-253). Australia: Charles Sturt University, Centre for Information Studies.

Hurst, S, Arulogun, OS, Owolabi, AO, Akinyemi, R, Uvere, E, Warth, S & Ovbiagele, B. 2015. Pretesting qualitative data collection procedures to facilitate methodological adherence and team building in Nigeria. *International Journal of Qualitative Method*s 14:53-64.

IAAB. 2015. *Handbook of international quality control, auditing, review, other assurance, and related services pronouncements*. New York: International Federation of Accountants.

Iacono, J, Brown, A & Holtham, C. 2009. Research methods – a case example of participant observation. *The Electronic Journal of Business Research Methods* 7(1):39-46.

ICA 1997. Guide for managing electronic records from an archival perspective. Available at: https://www.ica.org/sites/default/files/ICA%20Study%208%20guide_eng.pdf (Accessed 7 May 2018).

ICA. 2005. Electronic records: a workbook for archivists. Available at: https://www.ica.org/sites/default/files/ICA_Study-16-Electronic-records_EN.pdf (Accessed 5 May 2018).

ICA 2008. Principles and functional requirements for records in electronic office environments. Available at:

http://www.sa-fvg.archivi.beniculturali.it/fileadmin/materiali/ICA__Principles_and_Functional_Req uirements_for_Records_in_Electronic_Office_Environments.pdf (Accessed 8 May 2018).

ICA. 2013a. Principles and functional requirements for records in electronic office environments recordkeeping requirements for Database Based Business Systems. Available at: https://www.ica.org/sites/default/files/9.%20Recordkeeping%20Requirements%20for%20Database%20Based%20Business%20Systems.pdf (Accessed 3 October 2017).

ICA. 2013b. Recordkeeping requirements for database based business systems. Available at: https://www.ica.org/sites/default/files/9.%20Recordkeeping%20Requirements%20for%20Database%20Based%20Business%20Systems.pdf (Accessed 7 May 2018).

ICA/IRMT 2016. Understanding Digital Records Preservation Initiatives. Available at: https://www.ica.org/sites/default/files/Digital%20Preservation%20Initatives%20Module_0.pdf (Accessed 20 March 2018).

IFAC 2005. Proposed international education standard for professional accountants IES 8: competence requirements for audit professionals. Available at: https://www.iasplus.com/en/binary/ifac/0504educationies8.pdf (Accessed 26 April 2018).

InterPARES. 2005. The long-term preservation of authentic electronic records: findings of the InterPARES Project. Available at: http://www.imaginar.org/taller/dppd/DPPD/126%20pp%20InterPARES.pdf (Accessed 10 July 2016).

InterPARES. 2007. The InterPARES 2 project glossary. Available at: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_glossary.pdf (Accessed 20 May 2017).

InterPARES. 2008. International Research on Permanent Authentic Records in Electronic Systems (InterPARES) 2: Experiential, Interactive and Dynamic Records: Glossary. Available at: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_glossary.pdf (Accessed 20 January 2016).

InterPARES. 2015. Assessing information systems: a template for analysis. Available at: https://interparestrust.org/docs/file/TR04_20151228_InformationSystemsAnalysisTemplate_InternationalPlenary3_LiteratureReview.pdf (Accessed 12 July 2016).

InterPARES. 2016. Implementation of enterprise wide systems to manage trustworthy digital records in Botswana's public sector. Available at: https://interparestrust.org/assets/public/dissemination/AF04_20161231_EnterpriseRecordsManagementBotswana_LiteratureReview.pdf (Accessed 12 March 2018).

Illinois Department of Revenue. 1998. Electronic records and computer-assisted auditing. Available at: http://www.mtc.gov/uploadedFiles/Multistate_Tax_Commission/Audit_Program/Resource/Pub-107.pdf (Accessed 25 March 2018).

International Records Management Trust (IRMT). 1999. *Managing financial records*. London: IRMT.

International Records Management Trust (IRMT). 2001. *From accounting to accountability: managing financial records as a strategic resource in Namibia: a case study*. London: IRMT. Available at: http://www.irmt.org/documents/research_reports/accounting_recs/IRMT_acc_rec_namibia.PDF (Accessed 20 March 2016).

International Records Management Trust (IRMT). 2002a. *Evidence-Based Governance in the Electronic Age Case Study Financial Records and Information Systems in Tanzania*. London: IRMT. Available at: http://www.irmt.org/documents/research_reports/case_studies/financial_recs_case_studies/tanzania/IRMT_Finan_CS_Tanzania.pdf (Accessed 11 May 2016).

International Records Management Trust (IRMT). 2002b. *Evidence-based governance in the electronic age case study financial records systems in Nigeria*. London: IRMT. Available at: http://www.irmt.org/documents/research_reports/case_studies/financial_recs_case_studies/nigeria/IRMT_Finan_CS_Nigeria.pdf (Accessed 10 May 2016).

International Records Management Trust (IRMT) (2004a) *Evidence-based governance in the electronic age*. London: IRMT. Available at:

http://www.irmt.org/documents/research_reports/project_reports/Final%20DGF%20Report%20Revised.pdf (Accessed 24 April 2016).

International Records Management Trust (IRMT). (2004b). *E-records readiness tool*. London: IRMT. Available at: http://www.nationalarchives.gov.uk/rmcas/documentation/eRecordsReadinessTool_v2_Dec2004.pdf (Accessed 10 May 2016).

International Records Management Trust (IRMT). 2008. *Integrating records management in ICT system: good practice indicator*. IRMT: London, UK.

International Records Management Trust (IRMT). 2009. *Managing the creation, use and disposal of electronic records*. London: IRMT. Available at: http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%203.pdf (Accessed 12 October 2017).

InterPARES. 2005. The Long-term preservation of authentic electronic records: findings of the InterPARES project. Available at: http://www.imaginar.org/taller/dppd/DPPD/126%20pp%20InterPARES.pdf (Accessed 10 July 2016).

InterPARES 2016. AF04 Implementation of enterprise wide systems to manage trustworthy digital records in Botswana's public sector. Available at: https://interparestrust.org/assets/public/dissemination/AF04_20161231_EnterpriseRecordsManagementBotswana_LiteratureReview.pdf (Accessed 12 July 2017).

Institute of Internal Auditors. 2016. International standards for the professional practice of Internal Auditing (Standards*)*. Available at: https://na.theiia.org/standards-guidance/Public%20Documents/IPPF-Standards-2017.pdf (Accessed 11 May 2018).

Institute of Chartered Accountants in England and Wales. 2009. Uses and benefits of CAATs. Available at: https://www.icaew.com/-/media/corporate/files/about-icaew/what-we-do/127-a-guide-to-e-auditing.ashx (Accessed 10 May 2018).

Institute of Company Secretaries of India. 2014. Fundamentals of accounting and auditing. Available at:

https://www.icsi.edu/docs/webmodules/publications/FULL%20FAA%20PDF.pdf (Accessed 10 January 2017).

Isa, AM. 2009. Records management and the accountability of governance. PhD Thesis, University of Glasgow, Glasgow.

ISACA. 2008. *G3 Use of Computer-Assisted Audit Techniques* (CAATs). Available at: https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/CAATS/Use%20of%20CAATS.pdf (Accessed 10 May 2018).

ISACA. 2010. IT standards, guidelines, and tools and techniques for audit and assurance and control professionals. Available at: https://www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf (Accessed 10 May 2018).

Institute of Chartered Accountants in Australia. 2008. The Institute of Chartered Accountants in Australia 2008 Report to members, including full financial statements. Available at: https://www.charteredaccountantsanz.com/-/media/124bc0914f25442cb55cd3948f7b9ef4.ashx (Accessed 21 November 2018).

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

International Standards Organization (ISO) 23081-1: 2006: *Information and documentation – Records management processes metadata for records: Part 1: Principles*. Geneva: ISO.

International Standards Organization (ISO) 16175-2: 2011: *Information and documentation – Principles and functional requirements for records in electronic office environments: Part 2: Guidelines and functional requirements for digital records management systems*. Geneva: ISO.

International Standards Organization (ISO) 2016. *ISO 15489-1: Information and documentation - records management.* Geneva: ISO.

International Standards Organization (ISO) .2017: *ISO 15836*: *Information and documentation – the Dublin Core metadata element set: Part 1 core elements*. Geneva: ISO.

Jamshed, S. 2014. Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy* 5(4):87-88.

Jansen, A. 2014. Authenticity in records systems: emerging research in digital preservation, In (eds) Katre, D & Giaretta, D. 2014. *APA/C-DAC International conference on digital preservation and development of trusted digital repositories*, Aundh, Pune: Centre for Development of Advanced Computing.

Jantz, R. 2009. An institutional framework for creating authentic digital objects. Available at: http://www.ijdc.net/index.php/ijdc/article/viewFile/103/86 (Accessed 4 January 2017).

Jenkinson, H. 1937. A manual of archives administration. Available at: https://ia800806.us.archive.org/32/items/manualofarchivea00iljenk/manualofarchivea00iljenk.pdf (Accessed 23 December 2016).

Johnson, RB. 2014. Mixed methods research design and analysis with validity: a primer. Available at: http://www.ph-weingarten.de/zesa/Prof._Dr._Burke_Johnson_Mixed_Methods_PRIMER.pdf (Accessed 03 October 2016).

Johnson, B & Christenson, L. 2008. *Educational research: quantitative, qualitative and mixed approaches.* 3rd edition. California: Sage Publications Inc.

Johnson, RB & Onwuegbuzie, 2004. AJ. Mixed methods research: a research paradigm whose time has come. *Education Researcher 33* (7):14-16.

Johnston, JP & Bowen, DV. 2005. The benefits of electronic records management systems: a general review of published and unpublished cases. *Records management Journal* 15(3):131-140.

Jugder, N. 2016. The thematic analysis of interview data: an approach used to examine the influence of the market on curricular provision in Mongolian higher education institutions. Available at: http://hpp.education.leeds.ac.uk/wp-content/uploads/sites/131/2016/02/HPP2016-3-Jugder.pdf (Accessed 24 December 2017).

Jupp, V. 2006. *The Sage dictionary of social research methods*. London: Sage Publications

Kajornboon, AB. 2005. Using interviews as research instruments. Available at: http://www.culi.chula.ac.th/research/e-journal/bod/annabel.pdf (Accessed 12 June 2017).

Kalusopa, T. 2011. Developing an e-records readiness framework for labour organisations in Botswana. PhD Thesis, University of South Africa, Pretoria.

Kamatula, GA. 2010. Managing records at the University of Dar es Salaam – Tanzania. Masters Dissertation, University of Botswana. Gaborone.

Kanellou, A & Spathis, C. 2009. ERP systems and auditing: a review. Available at: https://www.researchgate.net/publication/274076878_ERP_Systems_and_Auditing_a_Review (Accessed 16 November 2018).

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

Katuu, S. 2016. Overview of the InterPARES Trust project in Africa: trusting records in an increasingly networked environment. *New Review of Information Networking* 21(2): 117-128.

Katuu, S & Ngoepe, M. 2015a. Managing digital heritage – an analysis of the education and training curriculum for Africa’s archives and records professionals. . *Digital Heritage* 2: 191-194.

Katuu, S & Ngoepe, M. 2015b. Managing digital records within South Africa’s legislative and regulatory framework. Proceedings of the 3rd International Conference on Cloud Security and Management ICCSM-2015 University of Washington Tacoma Washington USA 22-23 October 2015.

Katuu, S & Ngoepe, M. 2017. Education and training of archives and records management professionals in Africa. *UNESCO Newsletter* 22-27.

Keakopa, SM. 2007. The Management of electronic records in Botswana, Namibia and South Africa. PhD Thesis, University of London, London.

Keakopa, SM. 2008. Management of electronic mail: a challenge for archivists and records managers in Botswana, Namibia and South Africa. *ESARBICA Journal* 27:27-83.

Keakopa, SM. 2009. A critical review of the literature on electronic records management in the ESARBICA region. *ESARBICA Journal* 28:78-104.

Keakopa, SM. 2010. Overview of archival and records management developments in the ESARBICA region. *Archives and Manuscripts* 38(1):51-77.

Keetshabe, A. 2015. Development of ICT legal and regulatory framework in Botswana. Available at: http://slideplayer.com/slide/5965281/ (Accessed 16 July 2017).

Keetshabe, A. 2015. Developing cyber legislation in Botswana: an update. Available at: http://www.cit.co.bw/downloads/elegislation%20in%20botswana%20-%20keetshabe.pdf (Accessed 6 December 2016).

Kemoni, HN. 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* 19(3):190-203.

Kennedy-Clark, S. 2012. Design research and the solo higher degree research student: strategies to embed trustworthiness and validity into the research design. Available at: https://files.eric.ed.gov/fulltext/ED542294.pdf (Accessed 16 November 2018).

Kenosi, LS & Mosweu, O. 2018. A framework for a good recordkeeping system, in Ngulube, P (ed), *Handbook of Research on Heritage Management and Preservation*. Hershey PA: IGI Global: 213-234.

King, G, Keohane, RO & Verba. S. 1994. *Designing social inquiry*. Princeton: Princeton University Press.

Klein, M & Olbrech, M. 2011. Triangulation of qualitative and quantitative methods in panel peer review research. *International Journal for Cross-Disciplinary Subjects in Education* (IJCDSE) 2(2):342-348.

Knight, J. 2010. Survey on ICT attitudes to records and recordkeeping. Available at: https://futureproof.records.nsw.gov.au/wp-content/uploads/2008/12/ICT-attitudes-RM-Forum-presentation.pdf (Accessed 26 April 2018).

Knox, S & Burkard, AW. 2009. Qualitative research interviews. Available at: https://www.ncbi.nlm.nih.gov/pubmed/19579087 (Accessed 11 June 2017).

Kombo, DK & Tromp, DL. 2006. *Proposal and thesis writing: an introduction*. Nairobi: Pauline's Publications Africa.

Kothari, CR. 2004. *Research methodology – methods and techniques*. New Delhi: New Age International.

Kothari, CR & Garg, G. 2011. *Research methodology: methods and techniques*. New Delhi: New Age International (P) Limited, Publishers.

Krahn, K. 2012. Looking under the hood: unravelling the content, structure, and context of functional requirements for electronic recordkeeping systems. Masters Dissertation, University of Manitoba, Winnipeg,

Kritzinger, J. 2015. The application of analytical procedures in the audit process. Masters Dissertation, University of Pretoria, South Africa.

Kumar, R. 2005. *Research methodology: a step-by-step guide for beginners*. Los Angeles: Sage Publications.

Kumar, R. 2011. *Research Methodology: a step-by-step guide for beginners*. 3rd edition. London: Sage Publications.

Laudon, KC & Laudon, JP. 2014. *Management information systems: managing the digital firm*. 12th edition. San Francisco: Prentice Hall.

Latham, B. 2007. Sampling: what is it? Available at: https://docplayer.net/20989579-Sampling-what-is-it-quantitative-research-methods-engl-5377-spring-2007.html (Accessed 24 November 2018).

Latham, R. 2012. Information management advice 18 – managing records in business systems. Available at: https://www.informationstrategy.tas.gov.au/Records-Management-principles/Document%20Library%20%20Tools/Advice%2018%20Managing%20Records%20in%20Business%20Systems%20Part%205%20-%20Improving%20recordkeeping%20functionality.pdf (Accessed 16 November 2018).

Lauriault, TP, Barbara, LC, Taylor, DRF & Pulsifer PL. 2007. Today's data are part of tomorrow's research: archival issues in the sciences. *Archivaria* 64:123-179.

Leedy, PD & Ormrod, JE. 2005. *Practical research: planning and design*, New Jersey: Pearson Prentice.

Leedy, PD & Ormrod, JE. 2010. *Practical research: planning and design*. Boston: Pearson Education International.

Leedy, PD & Ormrod, JE. 2013. *Practical research: planning and design*, 10th edition. New Jersey: Pearson Education Inc.

Lemieux, VL. 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 (Accessed 5 August 2017).

Lester, F. 2005. On the theoretical, conceptual, and philosophical foundations for research in mathematics education. *ZDM* 37(6):457-467.

Levers, MD. 2013. Philosophical paradigms, grounded theory, and perspectives on emergence. *Sage Open* (October – December): 1-6.

Lewis, N. 2009. A guide to e-auditing. Available at: https://www.icaew.com/-/media/corporate/files/about-icaew/what-we-do/127-a-guide-to-e-auditing.ashx (Accessed 26 May 2018).

Library of Virginia. 2009. *Electronic records guidelines*. Available at: http://www.lva.virginia.gov/agencies/records/electronic/electronic-records-guidelines.pdf (Accessed 10 December 2016).

Lim, 2003. Digital signatures, certification authorities: certainty in the allocation of liability. Available at: http://www.commonlii.org/sg/journals/SGJlIntCompLaw/2003/9.pdf (Accessed 16 November 2018).

Lincoln, YS & Guba, EG. 1985. *Naturalistic inquiry*. Newbury Park CA: Sage Publications.

Little, A & Best, PJ. 2003. A framework for separation of duties in an SAP R/3 environment. *Managerial Auditing Journal* 18(5):419-430.

Livari, J, Parsons, J & Wand, Y. 2006. Research in information systems analysis and design: introduction to the special issue. Available at: https://pdfs.semanticscholar.org/112b/1cfef3687c56d9855481f2d21dd5b59ba590.pdf (Accessed 25 May 2018).

Livelton, T. 1991. Public records: a study in archival theory. Masters Dissertation, University of British Columbia, Vancouver.

Luyombya, D. 2010. Framework for effective public digital records management in Uganda. PhD Thesis, University College London, London.

Ma, J, Abie, H, Skramstad, T & Nygård, M. 2009. *Requirements for evidential value for the assessment of the trustworthiness of digital records over time*, in Proceedings of IEEE Symposium on trust, security, and privacy for pervasive applications, Macau SAR, China.

MacNeil, HM. 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.

MacNeil, H. 2000a. *Trusting records: legal, historical, and diplomatic perspectives*. Dordrecht: Kluwer Academic Publishers.

MacNeil, H. 2000b. Providing grounds for trust: developing conceptual requirements for the long-term preservation of authentic electronic records. *Archivaria*:52-59.

MacNeil, H. 2002. Providing grounds for trust II: The findings of the authenticity task force of InterPARES. *Archivaria* 54:24-58.

MacNeil, H. 2005. Picking our text: archival description, authenticity, and the archivist as editor. *The American Archivist* 68(2):264-278.

MacNeil, H. 2007. Archival theory and practice: between two paradigms. archives & social studies. *A Journal of Interdisciplinary Research* 1(1):517-545.

MacNeil, H & Gilliland-Swetland, A. 2005. Authenticity task force report. *In The Long-Term Preservation of Authentic Electronic Records: Finding of the InterPARES Project* (Eds.) Luciana Duranti. San Miniato: Archilab.

Mackenzie, NM. & Knipe, S. 2006. Research dilemmas: paradigms, methods and methodology. Available at: http://www.iier.org.au/iier16/mackenzie.html (Accessed 10 July 2017).

Maher, M & Akers, MD. 2003. Internal auditor participation in systems development projects. *Review of Business Information Systems* 7(2):11-20.

Makhura, MM & Du Toit, ASA. 2005. Records management and information user behaviour at SanParks: a case study. *Mousaion* 23(2):213-229.

Mak, B. 2012. On the uses of authenticity. *Archivaria* 73:1-17.

Makulilo, A. 2016. The admissibility of electronic evidence in Tanzania: new rules and case law. *Digital Evidence and Electronic Signature Law Review* 13:121-132.

Malanga, DF & Kamanga, CG. 2018. E-records readiness at Karonga District Council: applying IRMT E-records Readiness Assessment Framework. *Information Development*: 1-10.

Malasian Institute of Accountants. 2009. International Standard on Auditing ISA 500: Audit Evidence. Available at: http://www.mia.org.my/v1/downloads/psp/standards/ISA500.pdf (Accessed 01 March 2017).

Malemelo, F, Dube, A & David, R. 2013. Management of financial records at the Marondera municipality in Zimbabwe. *Journal of the South African Society of Archivists* 46:12-24.

Maluleka, JR. 2017. Acquisition, transfer and preservation of indigenous knowledge by traditional healers in the Limpopo Province of South Africa. PhD Thesis, University of South Africa, Pretoria.

Manewe-Sisa, P. 2013. Customer service at the Records Management Unit of the Ministry of Labour and Home Affairs in Botswana. Masters Dissertation, University of Botswana, Gaborone.

Manewe-Sisa, P, Mooko, PN & Mnjama, N. 2016. Customer service at the Records Management Unit of Botswana Ministry of Labour and Home Affairs. *African Journal of Library, Archives and Information Science* 26(2):155-165.

Marsden, P. 1997. When is the future? Comparative notes on the electronic record-keeping projects of the University of Pittsburgh and University of British Columbia. *Archivaria* 43:158-173.

Marutha, S. 2016. A framework to embed medical records management into the healthcare service delivery in Limpopo province of South Africa. PhD Thesis, University of South Africa, Pretoria.

Marutha, S & Ngulube, P. 2012. Electronic records management in the public health sector of the Limpopo province in South Africa. *Journal of the South African Society of Archivists* 45:39-67.

Maseh, EH. 2015. Records management readiness for open government in the Kenyan Judiciary. PhD Thesis, University of KwaZulu-Natal, Pietermaritzburg.

Mason, S. 2007. Authentic digital records: laying the foundation for evidence. *The Information Management Journal* September/October: 32-40.

Mathers, N, Fox, N & Hunn, A. 2002. Using interviews in a research project. Available at: http://web.simmons.edu/~tang2/courses/CUAcourses/lsc745/sp06/Interviews.pdf (Accessed 10 June 2017).

Mavodza, J. 2010. Knowledge management practices and the role of an academic library in a changing information environment: the case of the metropolitan college of New York, PhD Thesis, University of South Africa, Pretoria.

Maxwell, JA. 2013. *Qualitative research design: an interactive approach*. London: Sage Publications.

McCafferty, J. 2017. How internal auditors can gain data analytics experience. Available at: https://misti.com/internal-audit-insights/how-internal-auditors-can-gain-data-analytics-experience (Accessed 10 May 2018).

McDaniel, P. 2006. Authentication. Available at: https://pdfs.semanticscholar.org/dd3f/ba9b89a1f912a49463f2c9c28d9d726331a3.pdf (Accessed 20 March 2017).

McDonald, J. 1995. Managing information in an office systems environment: The IMOSA Project. *American Archivist* 58(2):142-153.

McKemmish, S. 2001. Placing records continuum theory and practice. *Archival Science* 1(4): 333-359.

McKemmish, S & Gilliland, A. 2013. Archival and recordkeeping research past, present and future. Available at: http://ozk.unizd.hr/rams/wp-content/uploads/2013/04/Chapter4.ResearchMethods-WilliamsonJohanson-2.pdf (Accessed 3 October 2017).

McLeod, J. 2012. On being part of the solution, not the problem: taking a proportionate approach to managing records. *Records Management Journal* 22(3):186-197.

McQueen, M. 2002. Language and power in profit/nonprofit relationships: A grounded theory of inter-sectoral collaboration. Available at: http://www.merylmcqueen.com/wp-content/uploads/2014/11/mcqueen-phdthesis-2002.pdf (Accessed 6 July 2017).

Meetoo, D & Temple, B. 2003. Issues in multi-method research: constructing self-care. *International Journal of Qualitative Methods* 2(3):1-21.

Meijer, AJ. 2001. Accountability in an information age: opportunities and risks for records management. *Archival Science* 1(4):361-372.

Meijer, AJ. 2003. Trust This Document! ICTs, Authentic records and accountability. *Archival Science* 3:275-290.

Mentz, 2014. An integrated audit evidence planning model to quantify the extent of audit evidence. PhD Thesis, University of South Africa.

Mertens, DM. 2010. *Research and evaluation in education and psychology: integrating diversity with quantitative, qualitative and mixed methods*. California: Sage publication.

Miller, A.G. 2001. Exhibiting integrity: archival diplomatics to study moving images. Masters Dissertation, University of British Columbia, Vancouver.

Ministry of Transport and Communication. 2017. Strategic refocusing of the national ICT sector. *Transcom Newsletter*. Gaborone: Ministry of Transport and Communication.

Minnesota State Archives. (2012). Electronic records management guidelines version 5. Available at: http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ElectronicRecordsManagementGuidelines032012_V5_Full_001.pdf (Accessed 20 June 2016).

Mir, FA & Banday, MT. 2012. Authentication of electronic records: limitations of Indian legal approach. *Journal of International Commercial Law and Technology* 7(3): 223-232.

Mnjama, N. 2014. Archival legislation and archival services in Africa, in (Eds), Sebina, PMM., Moahi, KH and Bwalya, KJ. 2014. *Digital access and e-government: perspectives from developing and emerging countries*. Hershey PA: IGI Global.

Mnjama, N & Wamukoya, J. 2004. *E-government and e-records management*. Paper presented at the SADC Workshop on E-government, Gaborone, Botswana, 14-16 April 2004.

Mnjama, N & Wamukoya, J. 2007. E-government and records management: an assessment tool for e-records readiness in government. *The Electronic Library* 25(3):274-284.

Moatlhodi, T. 2015. E-records readiness at the Ministry of Labour and Home Affairs. Masters Dissertation, University of Botswana, Gaborone.

Moglia, K, Alexander, K & Perez, P. 2011. Reflections on case studies, modelling and theory building. Paper presented at the 19th International Congress on Modelling and Simulation, Perth, Australia, 12–16 December 2011. Available at: https://www.mssanz.org.au/modsim2011/G3/moglia.pdf (Accessed 10 July 2017).

Mogull, R. n.d. Understanding and selecting a database activity monitoring solution. Available at: https://securosis.com/assets/library/reports/DAM-Whitepaper-final.pdf (Accessed 7 May 2018).

Mojapelo, MG. 2017. Contribution of selected chapter nine institutions to records management in the public sector in South Africa. Masters Dissertation, University of South Africa, Pretoria.

Moloi, J. 2009. E-records readiness in the public sector in Botswana. *ESARBICA Journal 28*: 105-127.

Moloi, J & Mutula, S. 2007. E-records management in an e-government setting in Botswana. *Information Development* 23(4):290-306.

Moorthy, M, Seetharaman, A, Mohamed, Z, Gopalan, M & San, LH. 2011. The impact of information technology on internal auditing. *African Journal of Business Management* 5(9): 3523-3539.

Moriarty, J. 2011. Qualitative methods overview. Available at: http://eprints.lse.ac.uk/41199/1/SSCR_Methods_Review_1-1.pdf (Accessed 25 July 2017).

Morrow, SL. 2005. Quality and trustworthiness in qualitative research in counseling psychology. *Journal of Counselling Psychology* 52(2): 250-260.

Morse, JM, Barrett, M, Mayan, M, Olson, K & Spiers, J. 2002. Verification strategies for establishing reliability and validity in qualitative research: *International Journal of Qualitative Methods* 1(2):13-22.

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

Mosweu, O, Bwalya, K & Mutshewa, A. 2016a. A probe into the factors for adoption and usage of electronic document and records management systems in the Botswana context. *Information Development*: 1-14.

Mosweu, O, Bwalya, K & Mutshewa, A. 2016b. Examining factors affecting the adoption and usage of document workflow management system (DWMS) using the UTAUT model: Case of Botswana. *Records Management Journal* 26(1): 1-30.

Mosweu, TL. 2012. Assessment of the court records management system in the delivery of justice at the Gaborone Magisterial District. Masters Dissertation, University of Botswana, Gaborone.

Mosweu, TL & Kenosi, L. 2018. Implementation of the Court Records Management System in the delivery of justice at the Gaborone Magisterial District, Botswana. *Records Management Journal* 28(3): 234-251.

Mostert, W. 2005. *The Electronic Communications and Transactions Act: Guide for Consumers, Businesses and Public Bodies.* Cape Town: Mostert Opperman Incorporated.

Motlhasedi, NY. 2012. E-records management at Botswana Training Authority. Masters Dissertation, University of Botswana, Gaborone.

Muchaonyerwa, N. 2017. Accessibility and security of digital records in the Office of the Premier in Eastern Cape, South Africa. *ESARBICA Journal* 36: 63-73.

Muchaonyerwa, N & Khayundi, F. 2014. The management of digital records in the Office of the Premier of the Eastern Cape Province, South Africa. *African Journal of Library and Information Science* 24(1): 41-52.

Mukwevho J & Jacobs, L. 2012. The importance of the quality of electronic records management in enhancing accountability in the South African public service: a case study of a National Department. *Mousaion* 30(2): 33-51.

Mulaudzi, M, Mukwevho, J & 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 (Accessed 2 July 2016).

Mulhall, A. 2003. In the field: notes on observation in qualitative research. *Journal of Advanced Nursing* 41(3):306-313.

Munetsi, N. 2011. Investigation into the state of digital records management in the provincial government of Eastern Cape: a case study of the office of the premier. Masters Dissertation, University of Fort Hare, Alice.

Namey, EE, Guest, G & Mitchell, ML. 2012. *Collecting qualitative data or applied research*. California: Sage.

NARA. 2005a. Records integrity and authenticity. Available at: https://www.nap.edu/read/11332/chapter/7 (Accessed 23 April 2018).

NARA. 2005b. NARA guidance on managing web records. Available at: https://www.archives.gov/records-mgmt/policy/managing-web-records.html (Accessed 21 December 2016).

NARA. 2018. Criteria for successfully managing permanent electronic records. Available at: https://www.archives.gov/files/records-mgmt/2019-perm-electronic-records-success-criteria.pdf (Accessed 6 May 2018).

National Archives of Australia. 2004. Digital recordkeeping guidelines for creating, managing and preserving digital records. Available at: http://mayaarbinaginting.weebly.com/uploads/1/0/6/1/10612501/digital_recordkeeping.pdf (Accessed 20 March 2016).

National Archives of Australia. 2015a. Digital information and records management capability matrix Skills and knowledge for Australian Government employees. Available at: http://www.naa.gov.au/naaresources/documents/capability-matrix.pdf (Accessed 20 May 2017).

National Archives of Australia. 2015b. Digital Continuity Policy 2020. Available at: http://www.naa.gov.au/Images/Digital-Continuity-2020-Policy_tcm16-93933.pdf (Accessed 7 May 2018).

National Archives of Australia. 2016. Implementation of digital continuity in the Australian government. Available at:

Governmenthttp://www.naa.gov.au/Images/Report%20to%20the%20Minister%202016%20%20Digital%20Transition%20and%20Digital%20Continuity%202020%20-%20FINAL_tcm16-95403.pdf (Accessed 18 May 2017).

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 (Accessed 13 May 2016).

National Archives of UK. 2011. Guide 8 Disposal of records. Available at: http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf (Accessed 25 March 2018).

National Archives of UK. 2012. Managing digital records without an electronic record management system. Available at: http://www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf (Accessed 26 March 2018).

National Archives of UK. 2017. Digital strategy. Available at: https://www.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf (Accessed 5 May 2018).

National Archives of South Africa. 2007. Records management policy manual. Available at: https://www.nationalarchives.gov.za/sites/default/files/RM%20Policy%20Manual_2.pdf (Accessed 12 May 2018).

National Archives of Namibia. 2007. Draft records management policies. Available at: http://www.opm.gov.na/documents/108506/160711/Draft+Records+Management+Policies+consolidated+200708.pdf/2eec4743-c898-4244-a408-0cac9ae87bc0?version=1.0 (Accessed 13 May 2018).

National Electronic Commerce Coordinating Council. 2004. Challenges in managing records in the 21st century. Available at: https://library.osu.edu/assets/Uploads/RecordsManagement/Challenges-in-21st-e-recs-neccc.pdf (Accessed 24 June 2016).

National Information Standards Organisation (NISO). 2004. Understanding metadata. Available at: http://www.niso.org/publications/press/UnderstandingMetadata.pdf (Accessed 10 June 2016).

National Archives of UK. 2011. Disposal of records. Available at: http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf (Accessed 24 September 2017).

Ndenje-Sichalwe, E. 2010. The significance of records management to fostering accountability in the public service reform programme. PhD Thesis, University of KwaZulu-Natal, Durban.

Ndenje-Sichalwe, E, Ngulube, P & Stilwell, C. 2011. Managing records as a strategic resource in the government ministries of Tanzania. *Information Development* 27(4): 264-279.

Nearon, BH. 2005. Foundations in auditing digital evidence. *The CPA Journal*. Available at: https://www.questia.com/magazine/1P3-780419261/foundations-in-auditing-and-digital-evidence (Accessed 20 July 2016).

Nengomasha, CT. 2009. A study of electronic records management in the Namibian public service in the context of e-government. PhD Thesis, University of Namibia, Windhoek.

Nengomasha, CT. 2013. The past, present and future of records and archives management in sub-Saharan Africa. *Journal of the South African Society of Archivists* 46:2-11.

Netshakhuma, NS. 2016. An exploration of the digitisation strategies of the liberation archives of the African National Congress in South Africa. Masters Dissertation, University of South Africa, Pretoria.

Neuman, WL. 2006. *Social research methods: qualitative and quantitative approaches*. Boston: Pearson Education Inc.

Neuman, WL. 2011. *Social research methods: qualitative and quantitative approaches*. Boston: Allyn and Bacon.

Neuman, WL. 2014. *Social research methods: qualitative and quantitative approaches*. Harlow: Pearson.

Ngidi, T. 2015. Management of medical records: a study at Princess Marina Hospital – Gaborone, Botswana. Masters Dissertation, University of Botswana, Gaborone.

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, South Africa 7:1-18.

Ngoepe, MS. 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.

Ngoepe, M. 2014. The role of records management as a tool to identify risks in the public sector in South Africa. *South African Journal of Information Management* 16(1):1-8.

Ngoepe, M. 2015. Deployment of open source electronic content management software in national government departments in South Africa. *Journal of Science & Technology Policy Management* 6(3):190-205.

Ngoepe, M & Keakopa, SM. 2011. An assessment of the state of national archival and records systems in the ESARBICA region. *Records Management Journal* 21(2):145-160.

Ngoepe, M & Makhubela, S. 2015. Justice delayed is justice denied: records management and the travesty of justice in South Africa. *Records Management Journal* 25(3): 288-305.

Ngoepe, M & Ngulube, P. 2013a. 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 32*:52-61.

Ngoepe, M & Ngulube, P. 2013b. An exploration of the role of records management in corporate governance in South Africa. *South African Journal of Information Management* 15(2):1-8.

Ngoepe, M & 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)* (24)2: 135–150.

Ngoepe, M & Ngulube, P. 2016. A framework to embed records management into the auditing process in the public sector in South Africa. *Information Development* 32(4): 890-903.

Ngoepe, M & 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* 44(1): 24-41.

Ngoepe, M & Van Der Walt, T. 2010. A framework for a records management programme: lessons from the Department of Cooperative Governance and Traditional Affairs in South Africa. *Mousaion* 28(2): 82–106.

Ngozwana. N. 2009. *Good Practice Guide for Public Accounts Committees in SADC*. Gaborone. SADC.

Ngulube, P. 2003. Preservation and Access to Public Records and Archives in South Africa. PhD Thesis, University of Natal, Pietermaritzburg.

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 & Library Review* 37(2):177-143.

Ngulube, P. 2013. Blending qualitative and quantitative research methods in library and information science in sub-Saharan Africa. *ESARBICA Journal: Journal of the Eastern and Southern Africa Regional Branch of the International Council on Archives* 32:3-16.

Ngulube, P. 2015. Trends in research methodological procedures used in knowledge management studies (2009 – 2013). *African Journal of Library, Archives and Information Science* 24(2): 125-143.

Ngulube, P. 2018. Overcoming the difficulties associated with using conceptual and theoretical frameworks in Heritage Studies. Available at: https://www.researchgate.net/publication/320471290_Overcoming_the_Difficulties_Associated_with_Using_Conceptual_and_Theoretical_Frameworks_in_Heritage_Studies (Accessed 28 May 2018).

Ngulube, P, Mathipa, ER & Gumbo, MT. 2015. Theoretical and conceptual frameworks in the social and management sciences. Available at: https://www.researchgate.net/publication/278961764_Theoretical_and_Conceptual_Frameworks_in_the_Social_and_Management_Sciences (Accessed 10 July 2017).

Ngulube, P, Mokwatlo, K & Ndwandwe, S. 2009. Utilization and prevalence of mixed methods research in library and information research in South Africa 2002-2008. *South African Journal of Libraries and Information Science* 75(2):105-116.

Ngulube. P & Ngulube. B. 2015. Mixed methods research in the South African Journal of Economic and Management Sciences: an investigation of trends in literature. *South African Journal of Economic and Management Sciences* 18(1):1-13.

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

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

Nkwe, N. 2012. E-Government: challenges and opportunities in Botswana. *International Journal of Humanities and Social Science* 2(17):13-48.

Nkala, SG, Ngulube, P & Mangena, BS. 2012. E-records readiness at National Archives of Zimbabwe. *Mousaion* 30(2):108-116.

Norman, LM, Tobedza, G & Swami, BN. 2015. Challenges faced by external auditors in Botswana. *International Journal of Social Sciences & Humanities* (IJSSH) 1(2):2395-5996.

Nowell, L. 2015. Pragmatism and integrated knowledge translation: exploring the compatibilities and tensions. Available at: http://onlinelibrary.wiley.com/doi/10.1002/nop2.30/epdf (Accessed 24 May 2016).

Nsibirwa, Z. 2007. Preservation of, and access to legal deposit materials at the Msunduzi Municipal Library. Masters Dissertation. University of KwaZulu-Natal, Pietermaritzburg.

Öberg, LM & Borglund, E. 2006. What are the characteristics of records? Available at: http://www.ltu.se/cms_fs/1.83857!/file/WhatAreTheCharacteristicsOfRecords.pdf (Accessed 20 December 2016).

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

Oganga, NC. 2016. Managing records for good governance in e-government environment: The Kenya experience. *Scholars Journal of Economics, Business and Management* 3(2):64-72.

Oginga, MG. 2013. The effect of adoption of computerised auditing on audit quality in Kenya. Masters Dissertation, University of Nairobi, Nairobi.

Ogunyemi. AO. 2014. Auditing and corruption in Nigeria: A Review of the legal weight of the Audit Act of 1956. *Historical Research Letter 15*:2224-3178.

Ojedokun, AA & Moahi, KH. 2006. Information and communication technology (ICT) systems in Botswana government departments. *African Journal of Library, Archives and Information Scienc*e 16(2):79-88.

Okello-Obura, C. 2011. Records and archives legal and policy frameworks in Uganda. Available at: http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1640&context=libphilprac (Accessed 25 July 2017).

Okello-Obura, C. 2012. Records and information management as a conduit to effective auditing. *ESARBICA Journal* 31:36-47.

Oloyede, R. 2017. Understanding digital/electronic signature framework in Nigeria. Available at: https://www.linkedin.com/pulse/understanding-digitalelectronic-signature-framework-nigeria-ridwan/ (Accessed 24 May 2018).

Ormerod, R. 2006. The history and ideas of pragmatism. *Journal of the Operational Research Society* 57:892-909.

O'Shea, G. 1996. Keeping electronic records: issues and strategies. Available at: http://www.netpac.com/provenance/vol1/no2/features/erecs1a.htm (Accessed 22 May 2017).

Padilla-Díaz, M. 2015. Phenomenology in educational qualitative research: philosophy as science or philosophical science? *International Journal of Educational Excellence* 1(2): 101-110.

Palmer, M. 2000. Records management and accountability versus corruption, fraud and maladministration. *Records Management Journal* 10(2): 61-72.

Parer, D. 2000. Archival legislation for commonwealth countries. Available at: http://www.acarm.org/oid%5Cdownloads%5C4%5C1_1_3_41_05_PM_Legislation%20Report.pdf (Accessed 5 December 2016).

Park, EG. 2001. Understanding "authenticity" in records and information management: analysing practitioner constructs. *American Archivist* 64:270-291.

Paré, G. 2004. Investigating information systems with positivist case research. *Communications of the Association for Information Systems* 13(18):233-264.

Pearce-Moses, R. 2005. A glossary of archival and records terminology. Available at: http://files.archivists.org/pubs/free/SAA-Glossary-2005.pdf (Accessed 20 May 2017).

Peshkar, P & Ghosekar, P. 2015. Role of database administrator in the IT industry. *International Journal of Emerging Research in Management &Technology* 4(12):41-44.

Pettigrew, KE & McKechnie, LEF. 2001. The use of theory in information science research. *Journal of the American Society for Information Science and Technology* 52(1):62-73.

Phiri, PM. 2016. Managing university records and documents in the world of governance audit and risk: case studies from South Africa and Malawi. PhD Thesis, University of Glasgow, Glasgow.

Photongsunan, S. 2010. Interpretive research in educational research. *Interpretive Paradigm in Educational Research*, October:1-4.

Piasecki, SJ. 1995. Legal admissibility of electronic records as evidence and implications for records management. *American Archivist* 58:54-64.

Pinielo, I. 2015. Auditor General reveals mess at Air Botswana. *Mmegi Newspaper Online* 13 February. Available at: http://www.mmegi.bw/index.php?aid=49185 (Accessed 3 July 2016).

Ponelis, SR. 2015. Using interpretive qualitative case studies for exploratory research in doctoral studies: a case of information systems research in small and medium enterprises. *International Journal of Doctoral Studies* 10:535-550.

PricewaterhouseCoopers. 2006. State of the internal audit profession study: Continuous auditing gains momentum. Available at:

http://www.pwc.com/us/en/internalaudit/assets/state_internal_audit_profession_study_06.pdf (Accessed 27 September 206).

Porter, B, Simon, J & Hatherly, J. 2003. *Principles of external auditing*, West Sussex: Wiley.

Powell, RR & Connaway, LS. 2004. *Basic research methods for librarians*. 4th edition. Westport: Libraries Unlimited.

Public Records Office. 2001. E-Government policy framework for electronic records management. Available at: http://www.nationalarchives.gov.uk/documents/egov_framework.pdf (Accessed 25 May 2018).

Public Record Office Victoria. 2003. Introduction to the Victorian electronic records strategy (VERS) PROS 99/007 (Version 2). Available at: https://www.prov.vic.gov.au/sites/default/files/2016-06/Intro_VERS.pdf (Accessed 5 May 2018).

Puttick, S, Van Esch, S & Kana, S. 2007. *The practice and principles of auditing*, Cape Town: Juta.

Quality Assurance Agency for Higher Education. 2015. UK quality code for higher education part A: Setting and maintaining academic standards. Available at: http://www.qaa.ac.uk/en/Publications/Documents/Doctoral-Degree-Characteristics-15.pdf (Accessed 3 July 2016).

RAFFA. 2003. Levels of attestation services defined-HANDOUT 3. Available at: https://www.scribd.com/document/156871960/3-Levels-of-Attestation-Services-Defined-HANDOUT-3 (Accessed 25 June 2018).

Rahman, MS. 2017. The advantages and disadvantages of using qualitative and quantitative approaches and methods in language. *Journal of Education and Learning* 6(1): 102-112.

Rakgailwane, MW. 2004. Audit profile. The Office of the Auditor General of Botswana. *International Journal of Government Auditing* October: 30-34

Randolph, JJ. 2009. A guide to writing the dissertation literature review. *Practical Assessment, Research and Evaluation* 14(3):1-13.

Reason, P. 2003. Pragmatist philosophy and action research readings and conversation with Richard Rorty. *Action Research* 1(1):103-123.

Reed, B. 2005. Records. in, S McKemmish., M Piggott. B Reed & F Upward (eds) *Archives: recordkeeping in society*. Wagg NSW: Centre for Information Studies.

Resnik, DB. 2015. What is ethics in research & why is it important? Available at: https://www.niehs.nih.gov/research/resources/bioethics/whatis/ (Accessed 7 June 2017).

Rezaei, N. 2013. Enterprise Resource Planning (ERP) software implementation impacts on the auditing activities. *Journal of Applied Business and Finance Researches* 2(3):90-96.

Richards, D. 2003. *The research project*. Available at: http://uncontrolled.info/Materialien/Essays/Research%20II.pdf (Accessed 27 July 2017).

Ritchie, J. 2003. The applications of qualitative methods to social research, in Ritchie, J & Lewis, J. 2003. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. London: Sage Publications.

Ritchie, J & Lewis, J. 2003. *Qualitative research practice: A guide for social science students and researchers*. London: Sage.

Ritchie, J, Spencer, L & O'Connor, L. 2003 Carrying out qualitative analysis, in Ritchie, J & Lewis, J. 2003. *Qualitative research practice: a guide for social science students and researchers*, London: Sage Publications.

Roeder, J, Eppard, P, Underwood, W & Lauriault, T. 2008. Authenticity, reliability and accuracy of digital records in the artistic, scientific and governmental sectors. Available at: http://www.interpares.org/ip2/display_file.cfm?doc=ip2_book_part_3_domain2_task_force.pdf (Accessed 16 November 2018).

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

Rogers, C. 2015b. *Virtual authenticity: authenticity of digital records from theory to practice*. Doctor of Philosophy, University of British Columbia, Vancouver.

Rogers, C. 2015c. Authenticity of digital records: a survey of professional practice. *Canadian Journal of Information and Library Science* 39(2):97-113.

Rogers, C. 2015d. Diplomatics of born digital documents – considering documentary form in a digital environment. *Records Management Journal* 25(1):6-20.

Rogers, C. 2016. A literature review of authenticity of records in digital systems: from 'machine readable' to records in the cloud. Available at: http://oaji.net/articles/2017/3932-1484337719.pdf (Accessed 23 March 2017).

Rogers, C & Tennis, J. 2013. Authenticity as a social contract: we are our records. iConference 2013. Proceedings Available at: https://www.ideals.illinois.edu/bitstream/handle/2142/42100/393.pdf?sequence=2 (Accessed 20 May 2017).

Rogers, R, Daum, P, Shaffer, E & Allen, A. 2013. Case Study 01 – British Columbia Institute of Technology (BCIT): Policies and procedures for preservation of digital records case study report. Available at: http://interpares.org/ip3/display_file.cfm?doc=ip3_canada_cs01_final_report.pdf (Accessed 16 November 2018).

Roratto, R & Dias, ED. 2014. Security information in production and operations: a study on audit trails in database systems. *Journal of Information Systems and Technology Management* 11(3): 717-734.

Ross, S. 1996. Consensus, communication and collaboration: fostering multidisciplinary cooperation in electronic records. In: *Proceedings of the DLM-Forum on Electronic Records*, Brussels, 18-20 December 1996. INSAR: European Archives News, Supplement II. Office for Official Publications of the European Communities, Luxembourg (1997) 330-336.

Rubin, HJ & Rubin IS. 2005. *Qualitative interviewing: the art of hearing data*. 2nd edition. Thousand Oaks, CA: Sage.

Runardotter, MC, Quisberg, H, Nilsson, J & Mirijamdotter, A. 2006. The information life cycle: issues in long-term digital preservation. Available at: https://www.researchgate.net/publication/228531497_The_information_life_cycle-issues_in_long-term_digital_preservation (Accessed 16 January 2017).

Ryan, B, Scapens, RW & Theobald, M. 2002. *Research method and methodology in finance accounting*. London: Thomson Learning.

Saman, WM & Haider, W.S. 2012. Electronic court records management: a case study. *Journal of e-Government Studies and Best Practices*: 1-11.

Saunders, M, Lewis, P & Thornhill, A. 2009. *Research methods for business students*. New York: Pearson Education Limited.

Saunders, MNK. Lewis, P & Thornhill, A. 2012. *Research methods for business students.* 6th edition. Harlow, England: Pearson Education.

Saurombe, NP. 2016. Public programming of public archives in the East and Southern Africa Regional Branch of the International Council on Archives (Esarbica): Towards an inclusive and integrated framework. PhD Thesis, University of South Africa, Pretoria.

Sayana, SE. 2003. Using CAATs to support IS audit. *Information Systems Control Journal* 1: 1-3.

Seymour, J. 2016. The modern records management program: an overview of electronic records management standards. Available at: https://onlinelibrary.wiley.com/doi/pdf/10.1002/bul2.2017.1720430212 (Accessed 12 May 2018).

Seymour, J. 2017. The modern records management program: an overview of electronic records management standards. Available at: http://onlinelibrary.wiley.com/doi/10.1002/bul2.2017.1720430212/epdf (Accessed 3 March 2018).

Shenton, AK. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information* 22:63-75.

Shweta, Y, Vikas, D & Naveen, G. 2016. Cyber threats and its impact on ecommerce sites. *International Journal of Control Theory and Applications* 9(41):805-812.

Singleton, RA & Straits, BC. 2010. *Approaches to social research*. New York: Oxford University Press.

Sisman, A. 2012. The e-Government concept and e-Government applications. Available at http://www.irma-international.org/viewtitle/64863/ (Accessed 21 November 2018).

Slack, F. 2001. Observation: perspectives on research methodologies for leisure managers. *Management Research News* 24(1):35-42.

Slife, BD & Williams, RN. 1995. *What's behind the research? Discovering hidden assumptions in the behavioural sciences*. Thousand Oaks, CA: Sage Publications.

South African Law Reform Commission. 2010. Review of the law of evidence. Available at: https://www.slideshare.net/wrrobinson/review-of-the-law-of-evidence-south-african-law-reform-commission (Accessed 29 November 2018).

South Carolina. 2007. Trustworthy information systems handbook. Available at: https://scdah.sc.gov/sites/default/files/Documents/Records%20Management%20(RM)/Electronic%20Records/Trustworthy%20Information%20Handbook/TISHandbook.pdf (Accessed 24 November 2018).

Sprehe, JT. 2002. Enterprise records management: strategies and solutions. Available at: http://ce.uoregon.edu/aim/ECM/rmstrategies.pdf (Accessed 20 December 2016).

Spyrelli, C. 2002. Electronic signatures: transatlantic bridge? An EU and US legal approach towards electronic authentication. *Journal of Information, Technology and Law*. Available at: http://egov.ufsc.br/portal/sites/default/files/anexos/27147-27157-1-PB.pdf (Accessed 11 January 2018).

Stair, RM & Reynolds, GW. 2006. *Principles of information systems: a managerial approach*. Boston: Thomason Learning Inc.

Stanfield, AR. 2016. The authentication of electronic evidence. PhD Thesis. Queensland University of Technology, Brisbane.

Stake, ER. 2010. *Qualitative research. Studying how things work*. New York: The Guilford Press.

Stake, RE. 1995. Case studies, in Denzin, NK & Lincoln, YS (eds.) *Handbook of qualitative research*. 2nd edition, Thousand Oaks: CA, Sage Publications.

State Comptroller of Israel. 2004. Israel: preservation of electronic records. Available at: http://www.intosaiitaudit.org/intoit_articles/23_p14top17.pdf (Accessed 20 March 2017).

State of Alaska. 2009. Building a trustworthy information system. Available at: https://archives.alaska.gov/pdfs/records_management/building_trustworthy_info_system_master.pdf (Accessed 13 November 2018).

State of New South Wales. 2002. Standard: No. 6 Standard on counter disaster strategies for records and recordkeeping systems. Available at: https://arp.nsw.gov.au/sites/default/files/Standard%20No%20%206%20-%20Counter%20Disaster%20Strategies.pdf (Accessed 7 May 2018).

State Records Office of Western Australia. 2015. State Records Office guideline: management of digital records. Available at: http://sro.wa.gov.au/sites/default/files/guideline_digital_records_v2.pdf (Accessed 13 November 2018).

Sullivan, KA. 2013. Building open government: the recordkeeping practices of federal agencies. Masters Dissertation, University of North Carolina, Chapel Hill.

Szívós, L & Orosz, I. 2014. The role of data authentication and security in the audit of financial statements. *Acta Polytechnica Hungarica* 11(8):161-176. Available at: http://www.uni-obuda.hu/journal/Szivos_Orosz_54.pdf (Accessed 23 March 2017).

Tafa, M. 2016. Understanding the Electronic Communications Act Part 1. Available at: http://www.armstrongs.bw/wp-content/uploads/2016/08/Edition-9-Understanding-The-Electronic-Communications-And-Transactions-Act-Moemedi-Tafa-4-Mar-2016.pdf (Accessed 21 April 2018).

Tafor, V. 2003. Digital technology – understanding the problems posed by information technology in generating and managing records from a third perspective. *ESARBICA Journal* 22:72-77.

Tahleho, T. 2016. Improving service delivery at the National University of Lesotho Library through knowledge sharing. Master of Information Science, University of South Africa, Pretoria.

Tank, MHK, Emley, SE & Whitaker, RD. 2013. A brief guide to using electronic signatures in securities transactions. *Practical Compliance & Risk Management for the Securities Industry* 23-34.

Tashakkori, A & Teddlie, C. 2003. *Handbook of mixed methods in social and behavioral research*. Thousand Oaks, CA: Sage.

Tashakkori, A & Teddlie, C. 2010. *Sage handbook of mixed methods in social and behavioural research*. Thousand Oaks, CA, Sage Publications.

Taylor-Powell, E & Renner, M. 2003. Analysing qualitative data. Available at: http://learningstore.uwex.edu/assets/pdfs/g3658-12.pdf (Accessed 20 May 2016).

Teddlie, C & Tashakkori, A. 2012. Common "Core" characteristics of mixed methods research: A review of critical issues and call for greater convergence. *American Behavioral Scientist* 56(6):774-788.

Teddlie, C & Yu, F. 2007. Mixed methods sampling: a typology with examples. *Journal of Mixed Methods Research* 1(1): 77-100.

Tennis, JT. 2008. Epistemology, theory, and methodology in knowledge organisation: toward a classification, metatheory, and research framework. *Knowledge Organisation* 35(2/3): 102-112.

Thanh, NC & Le Thanh, TT. 2015. The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science* 1(2):24-27.

Thibodeau, K. 2012. Wrestling with shape-shifters: perspectives on preserving memory in the digital age. Paper presented at the Memory of the World in the Digital Age: Digitization and Preservation, 26-28th September, Vancouver available at: http://www.ciscra.org/docs/UNESCO_MOW2012_Proceedings_FINAL_ENG_Compressed.pdf (Accessed 13 November 2018).

Thomas, DR & Hodges, I. 2010. Developing research aims and objectives. Available at: https://www.researchgate.net/profile/David_Thomas11/publication/224029399_Chapter_3_from_Designing_and_managing_your_research_project_Core_skills_for_social_and_health_research/links/00b7d520eee9676c77000000.pdf (Accessed 17 January 2017).

Thurston, A. 2015. Access to reliable public records as evidence for freedom of information in Commonwealth Africa. *The Commonwealth Journal of International Affairs:* 703-713.

Tongco, MDC. 2007. Purposive *sampling as a tool for informant selection*. Available at: http://journals.sfu.ca/era/index.php/era/article/viewFile/126/111 (Accessed 25 June 2018).

Trompeter, G & Wright, A. 2010. The world has changed: have analytical procedures? *Contemporary Accounting Research* 27(2): 669-700.

Tudor, CG, Gheorghe, M, Oancea, M & Şova, R. 2013. An analysis framework for defining the required IT&C competencies for the accounting profession. *Accounting and Management Information Systems* 12(4): 671-696.

Tutorials Point. 2015. Systems analysis and design. Available at: https://www.tutorialspoint.com/system_analysis_and_design/system_analysis_and_design_tutorial.pdf (Accessed 20 May 2018).

Uganda Law Reform Commission 2004. A study report on electronic transactions law. Available at: http://www.ulrc.go.ug/sites/default/files/ulrc_resources/Electronic%20Transactions%20Law%20body_0.pdf (Accessed 26 September 2016).

United Nations. 2004. Public sector transparency and accountability in selected Arab countries: policies and practices. Available at: https://publicadministration.un.org/publications/content/PDFs/E-Library%20Archives/2005%20Public%20Sector%20Transp%20and%20Accountability%20in%20SelArab%20Countries.pdf (Accessed 15 January 2018).

United Nations. 2006. Manual for the design and implementation of recordkeeping systems (DIRKS). Available at: https://archives.un.org/sites/archives.un.org/files/files/French%20files/Manual_for_the_Design_and_Implementation_of_Recordkeeping_Systems.pdf (Accessed 29 April 2018).

Uniting Church in Australia. 2017. Managing records in business systems guidelines. Available at: https://nswact.uca.org.au/media/4003/managing-records-in-business-systems-guideline.pdf (Accessed 5 October 2017).

University of South Africa (UNISA). 2016. Policy on research ethics. Available at: http://staffcmsys.Unisa.ac.za/cmsys/staff/contents/departments/res_policies/docs/Policy%20on%20Research%20Ethics%20-%20rev%20appr%20-%20Council%20-%2015.09.2016.pdf (Accessed 15 November 2016).

University of Southern California. 2018. Organizing your social sciences research paper: 9. the conclusion. Available at: http://libguides.usc.edu/writingguide/conclusion (Accessed 15 March 2018).

University of Tasmania. 2014. Records management guidelines. Available at: http://www.utas.edu.au/__data/assets/pdf_file/0006/29481/Records-Management-Guidelines.pdf (Accessed 21 November 2018).

University of Portsmouth. 2012. Document analysis. Available at: http://compass.port.ac.uk/UoP/file/ef9dd79a-2a94-4795-be23-f75eb40c8a11/1/Documentary%20and%20Content%20Analysis_IMSLRN.zip/page_02.htm (Accessed 21 November 2018).

Urquhart, C. 2015. Observation research techniques. *Journal of EAHIL* 11 (3):29-31, Available at: http://eahil.eu/wp-content/uploads/2015/09/29-31-Urquhart.pdf (Accessed 25 July 2017).

USAID. 2008. Integrated financial information systems: a practical guide. Available at: https://www.pempal.org/sites/pempal/files/attachments/PNADK595.pdf (Accessed 16 November 2018).

Valacich, JS & George, JF. 2017. *Modern systems analysis and design*. San Francisco: Pearson Education, Inc.

Venkatesh, V, Brown, SA & Bala, H. 2013. Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems. *MIS Quarterly* 37(1): 21-54.

WBI Evaluation Group. 2007. Documentary review. Available at: http://siteresources.worldbank.org/WBI/Resources/213798-1194538727144/11Final-Document_Review.pdf (Accessed 21 November 2018).

Wagner, C, Kawulich, B. & Garner, M. 2012. *Doing social research. A global Context*. London: McGraw-Hill Higher Education.

Waldo, J. 2006. On system design. Available at: https://scholar.harvard.edu/files/waldo/files/ps-2006-6.pdf (Accessed 3 December 2018).

Wallace, D. 2000. Recordkeeping metadata workshop. Available at: http://www.interpares.org/display_file.cfm?doc=ip1_dissemination_cons_amf-rkmw_proceedings_2000.pdf (Accessed 12 May 2018).

Walliman, N. 2006. *Social research methods*, London: Sage Publications.

Walliman, N. 2011. *Research methods: the basics*. New York: Routledge.

Wamukoya, J & Mutula, SM. 2005a. E-records management and governance in East and Southern Africa, *Malaysian Journal of Library & Information Science* 10(2): 67-83.

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

Wang, J. 2009. Challenges and strategies for managing digital records in a public organisation: findings from the TEAM China case study," in *Proceedings of the InterPARES 3 International Symposium*, 4-5 June 2009, Seoul, South Korea (Seoul: Sungkyunkwan University, 2009): 243-277.

Watney, M. 2009. Admissibility of electronic evidence in criminal proceedings: an outline of the South African legal position. Available at: https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/watney/watney.pdf (Accessed 18 January 2017).

Wato, R. 2006. E-records readiness in the Esarbica: challenges and the way forward. *ESARBICA Journal* 25: 69-83.

Wellington, J. 2013. Searching for 'doctorateness'. *Studies in Higher Education* 38(10): 1490-1503.

Whittington, OR & Pany, K. 2010. *Principles of auditing and other assurance services*. New York: McGraw-Hill.

Williams, C. 2006. *Managing archives: foundations, principles and practice*. Hartcourt: Chandos Publishing (Oxford) Limited.Williams, G. 2014. *Poor records management affects service delivery*. Gaborone: Botswana Press Agency.

Williams, M & May, T. 1996. *Introduction to the philosophy of social research*. London: UCL Press.

Williamson, K. 2013. Research concepts, in Williamson K & Johnson G (eds), *Research methods: information, systems and contexts*. Prahran: Tilde.

Willis, JW. 2007. *Foundations of qualitative research: interpretive and critical approaches*. London: Sage.

Wisdom, JP, Cavaleri, MA, Onwuegbuzie, AJ & Green, CA. 2012. Methodological reporting in qualitative, quantitative, and mixed methods health services research articles. *HSR: Health Services Research* 47(2):721-745.

World Bank/IRMT. 2000. Managing records as the basis for effective service delivery and public accountability in development: An introduction to core principles for staff of the World Bank and its partners. Available at: http://siteresources.worldbank.org/EXTARCHIVES/Resources/Core%20Principles.pdf (Accessed 22 May 2018).

Xiaomi, A. 2003. An integrated approach to records management. *Information Management Journal* July/August: 24-30.

Xie, A. 2013. Preserving digital records: InterPARES findings and developments, in Lemieux, V. 2013 (ed). *Financial Analysis and Risk Management.* Verlag Berlin Heidelberg: Springer.

Xie, SL. 2011. Building foundations for digital records forensics: a comparative study of the concept of reproduction in digital records management and digital forensics. *The American Archivist* 7: 576-599.

Yeasmin, S & Rahman, KF. 2012. Triangulation research method as the tool of social science research. *BUP Journal* 1(1): 154-163.

Yin, RK. 2009. *Case study research: design and methods*. 4th edition. New Delhi: Sage Publications.

Zinyama, T. 2013. Efficiency and effectiveness in public sector auditing: an evaluation of the Comptroller and Auditor General's performance in Zimbabwe from 1999 to 2012. *International Journal of Humanities and Social Science* 3(7): 267-282.

APPENDICES

Appendix 1: Phases of the Audit Process Using ISA Standards

Engagement activities
ISA 200: Overall objectives of the auditor and the conduct of the audit ISA 210: Agreeing the terms of the audit engagement ISA 220: Quality control for the audit of the financial statements

Planning the audit
ISA 300: Planning the audit of the financial statements ISA 315: Understanding the entity and its environment and identifying and assessing the risks of material misstatement ISA 320: Setting materiality ISA 330: The auditor's responses to assessed risks ISAs 240 & 250: The auditor’s responsibility relating to fraud and the consideration of laws and regulations

Obtaining audit evidence
ISA 230: Audit documentation ISA 330: The auditor's responses to assessed risks ISAs 500, 501, 505, 510, 520, 530, 540, 560, 570, 580, 600, 610 & 620: Obtaining audit evidence ISA 450: Evaluating misstatements identified during the audit

Concluding and reporting
ISAs 700, 705, 706, 710 & 720: Forming an opinion and reporting on the financial statements ISAs 260 & 265: Communication with those charged with governance, including internal control deficiencies

Appendix 2: Application for Research Permit at MFED

P O Box 26071
GABORONE

9 October 2017

The Permanent Secretary
Ministry of Finance and Economic Development
Private Bag 008
GABRORONE

Dear Sir/Madam

APPLICATION FOR PERMISSION TO COLLECT DATA

I am a Doctoral student, Student No: 58553304, in the Department of Information Sciences at the University of South Africa (UNISA). I am conducting research on "*Authenticating digital records in Government Accounting System to support auditing processes in the public sector of Botswana*." At the end, the study aims to propose a framework for ensuring that authentic reliable digital records created and stored in GABS are able to support auditing processes in the public sector of Botswana. An approved research proposal is attached in order to enable you to appreciate the proposed study in totality.

I am therefore writing requesting for permission to collect data in your ministry. Please find attached an Ethical Clearance Letter issued by UNISA's Research Ethics Review Committee, UNISA Ethical Clearance number 2017_OMosweu_58553304_001.

I would like to collect data from Department of Corporate Services (MFED), Accountant General's Department (AGD) and the Department of Internal Audit (DIA), specifically from the following officers;

a. Records Manager (1)
b. Chief/Principal Internal Auditors (3)
c. Chief Finance Officer - Systems Support (1)
d. Chief/Principal Systems Analysts (3)

I would like to interview the stated officers. I would also like to collect data through system analysis of GABS and controls in place for the system. My supervisor is Professor Ngoepe, UNISA, ngoepms@Unisa.ac.za

Thanks for your anticipated assistance

Yours faithfully

____

Olefhile Mosweu (Mr.)
National ID: 563 419 403

Appendix 3: Application for Research Permit at Office of the Auditor General

P O Box 26071
GABORONE

29 September 2017

Auditor General
Office of the Auditor General
Private Bag 0010
GABRORONE

Dear Sir/Madam

APPLICATION FOR PERMISSION TO COLLECT DATA

I am a Doctoral student, Student No: 58553304, in the Department of Information Sciences at the University of South Africa (UNISA). I am conducting research on "*Authenticating digital records in Government Accounting System to support auditing processes in the public sector of Botswana*." At the end, the study aims to develop a framework for to propose a framework for ensuring that authentic reliable digital records are created and stored in GABS to support auditing processes in the public sector of Botswana.

I am therefore writing requesting for permission to collect data in your ministry. Please find attached an Ethical Clearance Letter issued by UNISA's Research Ethics Review Committee, UNISA Ethical Clearance number 2017_OMosweu_58553304_001.

I would like to collect data from the Office of the Auditor General, specifically from the following officers;

Chief Auditor: Central Government (1)

Principal Auditor: Information Systems (2)

Principal Audit Officer (Information System) (1)

Records Manager/Head of Records Management (1)

I would like to interview the stated officers. I would also like to collect data through system analysis GABS and controls in place for the system. My supervisor is Professor Ngoepe, Department of Information Science, University of South Africa, ngoepms@Unisa.ac.za

Thanks for your anticipated assistance

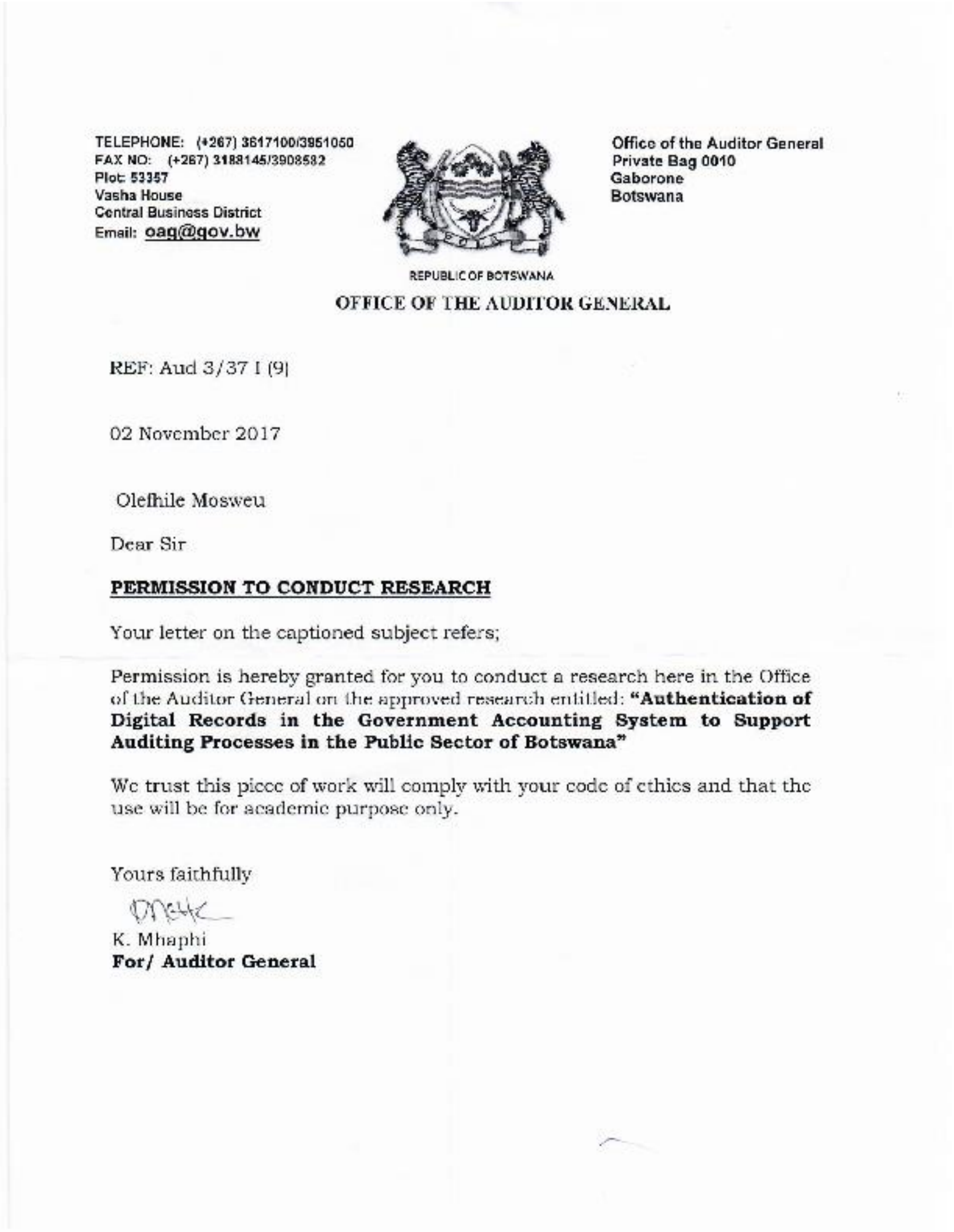
Yours faithfully

____

Olefhile Mosweu (Mr.)

National ID: 563 419 403

Appendix 4: Research Permit: Office of The Auditor General of Botswana



TELEPHONE: (+267) 3617100/3951050
FAX NO: (+267) 3188145/3908582
Plot: 53357
Vasha House
Central Business District
Email: oag@gov.bw

Office of the Auditor General
Private Bag 0010
Gaborone
Botswana

REPUBLIC OF BOTSWANA

OFFICE OF THE AUDITOR GENERAL

REF: Aud 3/37 I (9)

02 November 2017

Olefhile Mosweu

Dear Sir

PERMISSION TO CONDUCT RESEARCH

Your letter on the captioned subject refers;

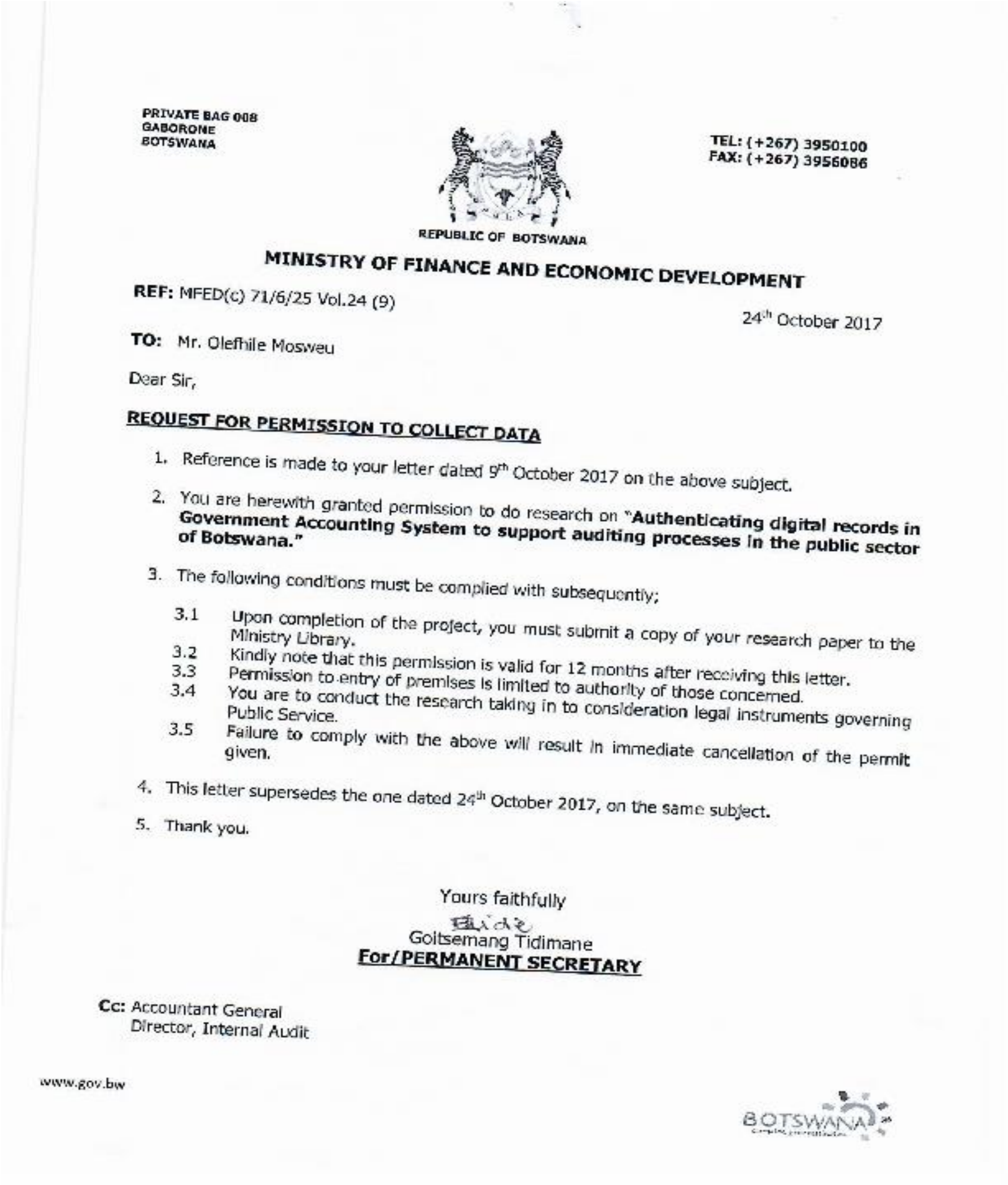
Permission is hereby granted for you to conduct a research here in the Office of the Auditor General on the approved research entitled: **"Authentication of Digital Records in the Government Accounting System to Support Auditing Processes in the Public Sector of Botswana"**

We trust this piece of work will comply with your code of ethics and that the use will be for academic purpose only.

Yours faithfully

K. Mhaphi
For/ Auditor General

Appendix 5: Research Permit: Ministry of Finance and Economic Development



PRIVATE BAG 008
GABORONE
BOTSWANA

TEL: (+267) 3950100
FAX: (+267) 3956086

REPUBLIC OF BOTSWANA

MINISTRY OF FINANCE AND ECONOMIC DEVELOPMENT

REF: MFED(c) 71/6/25 Vol.24 (9)

24th October 2017

TO: Mr. Olefhile Mosweu

Dear Sir,

REQUEST FOR PERMISSION TO COLLECT DATA

1. Reference is made to your letter dated 9th October 2017 on the above subject.
2. You are herewith granted permission to do research on **"Authenticating digital records in Government Accounting System to support auditing processes in the public sector of Botswana."**
3. The following conditions must be complied with subsequently;

   3.1 Upon completion of the project, you must submit a copy of your research paper to the Ministry Library.
   3.2 Kindly note that this permission is valid for 12 months after receiving this letter.
   3.3 Permission to entry of premises is limited to authority of those concerned.
   3.4 You are to conduct the research taking in to consideration legal instruments governing Public Service.
   3.5 Failure to comply with the above will result in immediate cancellation of the permit given.

4. This letter supersedes the one dated 24th October 2017, on the same subject.
5. Thank you.

Yours faithfully

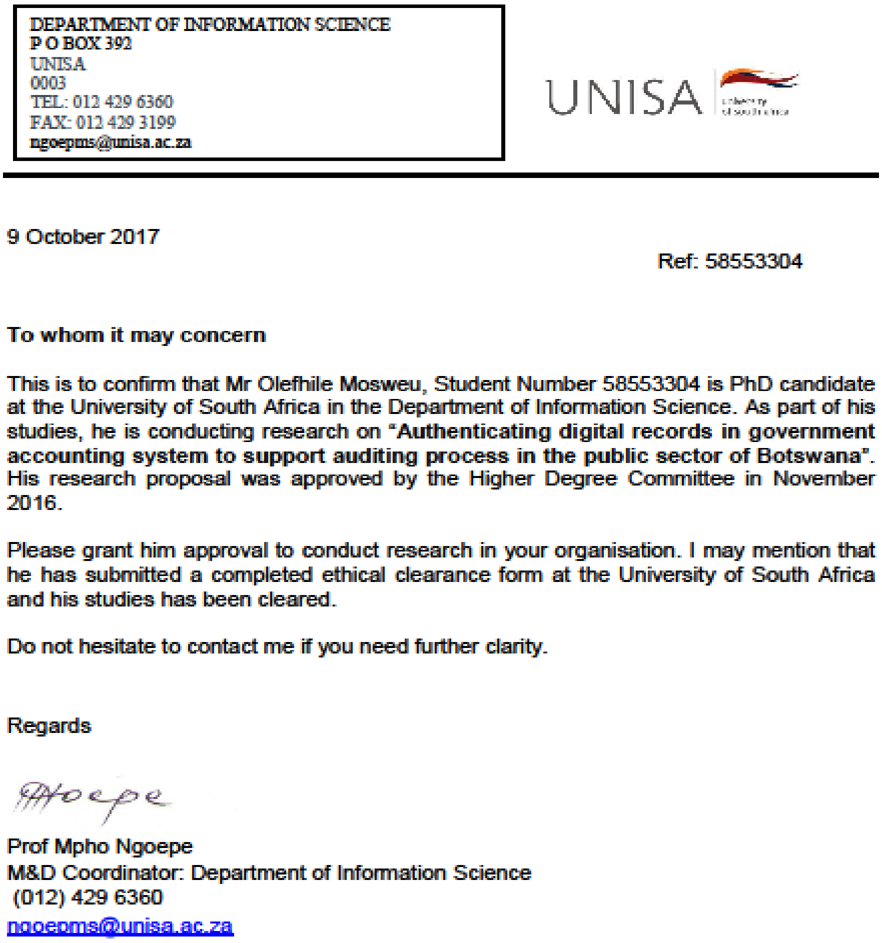
Goitsemang Tidimane
For/PERMANENT SECRETARY

Cc: Accountant General
Director, Internal Audit

www.gov.bw

BOTSWANA

Appendix 6: Letter of Introduction by Promoter



DEPARTMENT OF INFORMATION SCIENCE
P O BOX 392
UNISA
0003
TEL: 012 429 6360
FAX: 012 429 3199
ngoepms@unisa.ac.za

9 October 2017

Ref: 58553304

To whom it may concern

This is to confirm that Mr Olefhile Mosweu, Student Number 58553304 is PhD candidate at the University of South Africa in the Department of Information Science. As part of his studies, he is conducting research on **"Authenticating digital records in government accounting system to support auditing process in the public sector of Botswana"**. His research proposal was approved by the Higher Degree Committee in November 2016.

Please grant him approval to conduct research in your organisation. I may mention that he has submitted a completed ethical clearance form at the University of South Africa and his studies has been cleared.

Do not hesitate to contact me if you need further clarity.

Regards

Ngoepe

Prof Mpho Ngoepe
M&D Coordinator: Department of Information Science
(012) 429 6360
ngoepms@unisa.ac.za

Appendix 7: Study Ethical Clearance by Unisa Ethics Committee

DEPARTMENT OF INFORMATION SCIENCE RESEARCH ETHICS REVIEW COMMITTEE

Date: 11 August 2017

Ref #: 2017_OMosweu_58553304_001

Name of applicant: O Mosweu

Student #:X

Dear O Mosweu,

Decision: Ethics Approval

Name: Title and name of principle applicant, address, e-mail address, and phone number O Mosweu, Unisa Information Science, 58553304@mylife.Unisa.ac.za; and +26772264000

Proposal: Authenticating digital records in government accounting systems to support auditing processes in the public sector of Botswana.

Qualification: PHD in Information Science

Thank you for the application for research ethics clearance by the Department of Information Science Research Ethics Review Committee for the above mentioned research. Final approval is granted for *4 years.*

For full approval: *The application was reviewed in compliance with the Unisa Policy on* Research Ethics by the Department of Information Science Research Ethics Review Committee on 11 August 2017.

The proposed research may now commence with the proviso that:

1) *The researcher/s will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.*
2) *Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Department of information Science Ethics Review Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially if those changes affect any of the study-related risks for the research participants.*

3) The researcher will ensure that the research project adheres to any applicable national legislation, professional codes of conduct, institutional guidelines and scientific standards relevant to the specific field of study.

Note:

The reference number 2017_OMosweu_58553304_001 *should be clearly indicated on all forms* of communication [e.g. Webmail, E-mail messages, letters] with the intended research participants, as well as with the Department of Information Science RERC.

Kind regards

Signature

Dr Isabel Schellnack-Kelly

Department of Information Science Research Ethics Review Committee

012 429 6936

Appendix 8: Interview Guide – ICT Specialists: Department of Information Technology

"A FRAMEWORK TO AUTHENTICATE RECORDS IN A GOVERNMENT ACCOUNTING SYSTEM IN BOTSWANA TO SUPPORT THE AUDITING PROCESS"

My name is Olefhile Mosweu, a PhD student in the Department of Information Science, University of South Africa (UNISA). I am conducting an empirical study on "*authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana".* My student number is 58553304. The study is about the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. The study would also propose a framework for ensuring that authentic reliable records are created and stored in GABS to support auditing processes in the public sector of Botswana.

The findings of the study stand to benefit the Government of Botswana in terms of creating and maintaining authentic reliable digital accounting records for decision making, accountability purposes and meeting the requirements of auditors of financial statements. This is particularly crucial in an era where the Government of Botswana is implementing its e-Government strategy whose services produce digital records. The said records have to conform to appropriate legislation and standards in order to be accepted by auditors as electronic evidence in the audit process.

The confidentiality of study participants will be ensured on the data collected. Participation is voluntary and the study is purely for academic purposes. In order for participants to remain anonymous, names are not required. The interviews are intended to seek opinions on the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. You can call me at +267 72569181/+267 3688 227 or email me at olfmos@gmail.com if you have questions concerning this study. You can also get in touch with my supervisor, Professor Ngoepe, UNISA at ngoepms@Unisa.ac.za if you need further clarity.

Thank you in advance

Yours faithfully

____

Olefhile Mosweu

I hereby give consent for my participation in this study and that the information I give out be ONLY be used for purposes of accomplishing the purpose of this study. The information collected will be treated with utmost confidentiality and will remain anonymous. Please append your signature to confirm your consent to taking part in the study.

Participant signature: ___________ Date: _______________

Participant biographical profile (Please tick the appropriate response)

1. Gender

a. Male_____________b. Female____________

2. Age

a. 20 – 30 years ( )
b. 31 – 40 years ( )
c. 41 – 50 years ( )
d. 51 – 60 years ( )

3. Educational background

a. Diploma in Computer Science/Studies ( )
b. Degree Computer Science/Studies ( )

c. Masters' Degree Computer Science/Studies ( )

d. PhD Computer Science/Studies ( )

e. Other: ________________________________ (Please specify)

4. Work experience

a. 2 - 6 years ( )

b. 7 - 11 years ( )

c. 12 -16 years ( )

d. 17 – 21 years ( )

e. 22 - 26 years ( )

f. More than 27 years ( )

5. Job designation: ____________________________________ (Please write in full)

A. Objective 2: To find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

6. Digital accounting records are created and stored in GABS. What functionalities does GABS have to ensure that it creates and maintains authentic reliable digital accounting records in the system?

7. 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?

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

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 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.		

B. Objective 3: To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS.

9. What specific technical competencies do ICT specialists need to authenticate/establish and maintain the authenticity and reliability of digital records created and stored in GABS?

10. What would be the impact of inadequate competencies and skills for ICT specialists in determining the authenticity of digital records?

11. To what extent is the current ICT infrastructure supportive of the creation and maintenance of authentic records in GABS? Please explain your answer.

C. Objective 4: To determine how digital records created and stored through GABS are managed as authentic and reliable to support auditing processes in the public sector of Botswana.

12. Are the records directly generated in the system or digitized/scanned into the system? Please explain further.

13. Accounting transactions done through GABS produce digital records, what metadata exists in the system to ensure the management across their life cycle?

14. The Government of Botswana's Financial Instructions and Procedures specifies various retention periods for accounting records. Have records retention periods been captured into GABS to guide records retention and disposal in the system?

15. If NO, to the question above, is there a backup system in place to maintain digital accounting records in the system authentic and reliable since the system was implemented in 2005? Please explain in detail.

17. What management challenges are experienced in the ongoing management of digital accounting records in GABS, if any?

18. If YES, how have they been resolved?

19. Is GABS integrated with other information systems (e.g. digital records management system) for the authentic management of digital records? Please explain further.

21. If NO, does it have the capability to be integrated with such systems?

22. What General IT and system application controls are in place to protect the authenticity of records in GABS?

23. What recommendations can you propose related to the creation and maintenance of authentic digital accounting records with integrity in GABS?

Appendix 9: Interview Schedule: ICT Specialists/Gabs System Support: Department of Accountant General

"A FRAMEWORK TO AUTHENTICATE RECORDS IN A GOVERNMENT ACCOUNTING SYSTEM IN BOTSWANA TO SUPPORT THE AUDITING PROCESS"

My name is **Olefhile Mosweu**, a PhD student in the Department of Information Science, University of South Africa (Unisa). My student number is **58553304**. I am conducting an empirical study on "***A framework to authenticate records in a Government Accounting System in Botswana to support the auditing process".*** The study is about the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. The study would also propose a framework for ensuring that authentic reliable records are created and stored in GABS to support auditing processes in the public sector of Botswana.

The findings of the study stand to benefit the Government of Botswana in terms of creating and maintaining authentic reliable digital accounting records for decision making, accountability purposes and meeting the requirements of auditors of financial statements. This is particularly crucial in an era where the Government of Botswana is implementing its e-Government strategy whose services produce digital records. The said records have to conform to appropriate legislation and standards in order to be accepted by auditors as electronic evidence in the audit process.

The confidentiality of study participants will be ensured on the data collected. Participation is voluntary and the study is purely for academic purposes. In order for participants to remain anonymous, names are not required. The interviews are intended to seek opinions on the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. You can call me at +267 72569181/+267 3688 227 or email me at olfmos@gmail.com if you have questions concerning this study. You can also get in touch with my supervisor, Professor Ngoepe, UNISA at ngoepms@Unisa.ac.za if you need further clarity.

Thank you in advance

Yours faithfully

____

Olefhile Mosweu

I hereby give consent for my participation in this study and that the information I give out be ONLY be used for purposes of accomplishing the purpose of this study. Please append your signature to confirm your consent to taking part in the study.

Participant signature: __________ **Date**: ______________

Participant biographical profile (Please tick the appropriate response)

1. **Gender**

a. Male____________b. Female___________

2. **Age**

a. 20 – 30 years ( )
b. 31 – 40 years ( )
c. 41 – 50 years ( )
d. 51 – 60 years ( )

3. **Educational background**

a. Diploma in Computer Science/Studies ( )
b. Degree Computer Science/Studies ( )

c. Masters’ Degree Computer Science/Studies ( )

d. PhD Computer Science/Studies ( )

e. Other: __________________________________ (Please specify)

4. **Work experience**

a. 2 - 6 years ( )

b. 7 - 11 years ( )

c. 12 -16 years ( )

d. 17 – 21 years ( )

e. 22 - 26 years ( )

f. More than 27 years ( )

5. **Job designation**: _______________________________________ (Please write in full)

A. Objective 2: To find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

6. Digital accounting records are created and stored in GABS. What functionalities does GABS have to ensure that it creates and maintains authentic reliable digital accounting records in the system?

7. 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?

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

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 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		

B. Objective 3: To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate/establish the authenticity and reliability of digital records created and stored in GABS.

9. What specific technical competencies do ICT specialists need to authenticate/establish and maintain the authenticity and reliability of digital records created and stored in GABS?

10. What would be the impact of inadequate competencies and skills for ICT specialists in ascertaining the authenticity of digital records?

11. To what extent is the current ICT infrastructure supportive of the creation, protection and maintenance of digital accounting records with integrity in GABS? Please explain your answer.

C. Objective 4: To determine how digital records created and stored through GABS are managed and preserved as authentic and reliable to support auditing processes in the public sector of Botswana.

12. Are the records directly generated in the system or digitized/scanned into the system?
Please explain further.

13. Accounting transactions done through GABS produce digital records, what metadata exists in the system to ensure the management across their life cycle?

14. The Government of Botswana's Financial Instructions and Procedures specifies various retention periods for accounting records. Have records retention periods been captured into GABS to guide records retention and disposal in the system?

15. What preservation challenges are experienced in the ongoing management of digital accounting records in GABS, if any?

17. Is GABS integrated with other information systems? If yes, what are they?

18. What recommendations can you propose for the maintenance of authentic digital accounting records created and stored in GABS?

Appendix 10: MFED Records Managers

"A FRAMEWORK TO AUTHENTICATE RECORDS IN A GOVERNMENT ACCOUNTING SYSTEM IN BOTSWANA TO SUPPORT THE AUDITING PROCESS"

My name is **Olefhile Mosweu**, a PhD student in the Department of Information Science, University of South Africa (Unisa). My student number is **58553304**. I am conducting an empirical study on "***A framework to authenticate records in a Government Accounting System in Botswana to support the auditing process".*** The study is about the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. The study would also propose a framework for ensuring that authentic reliable records are created and stored in GABS to support auditing processes in the public sector of Botswana.

The findings of the study stand to benefit the Government of Botswana in terms of creating and maintaining authentic reliable digital accounting records for decision making, accountability purposes and meeting the requirements of auditors of financial statements. This is particularly crucial in an era where the Government of Botswana is implementing its e-Government strategy whose services produce digital records. The said records have to conform to appropriate legislation and standards in order to be accepted by auditors as electronic evidence in the audit process.

The confidentiality of study participants will be ensured on the data collected. Participation is voluntary and the study is purely for academic purposes. In order for participants to remain anonymous, names are not required. The interviews are intended to seek opinions on the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. You can call me at +267 72569181/+267 3688 227 or email me at olfmos@gmail.com if you have questions concerning this study. You can also get in touch with my supervisor, Professor Ngoepe, UNISA at ngoepms@Unisa.ac.za if you need further clarity.

Thank you in advance

Yours faithfully

____

Olefhile Mosweu

I hereby give consent for my participation in this study and that the information I give out be ONLY be used for purposes of accomplishing the purpose of this study. Please append your signature to confirm your consent to taking part in the study.

Participant signature: __________ **Date**: ______________

Interview schedule

Objective 1: To analyse the legislative framework for the creation of authentic reliable digital records stored in Government Accounting and Budgeting System (GABS) in support of auditing processes in the public sector of Botswana.

1. What standards and guidelines are in place to guide and promote the creation and maintenance of authentic digital accounting records in GABS? Please explain.

2. To what extent are issues of digital records authenticity over time adequately addressed by available legislation and policies that regulate financial records management?

Objective 2: To find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

5. 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.

Objective 3: To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS.

6. What level of training/qualifications do you have in records management?

7. What competencies do records management personnel need to declare that digital records (data) created and stored in GABS have their integrity and identity (authenticity) maintained over time?

8. What would be the impact of inadequate ICT competencies and skills for records managers in ascertaining the authenticity of digital records?

Objective 4: To determine how digital records created and stored through GABS are managed and preserved as authentic and reliable to support auditing processes in the public sector of Botswana.

9. Has BNARS issued records disposal guidelines for the management of digital records in the public sector? Please explain your answer.

10. What digital management strategies are in place to ensure that public sector digital records are preserved for as long as needed?

11. What recommendations can you propose to ensure that records in GABS are created and maintained? Please offer as many recommendations as possible.

Appendix 11: Interview Schedule: BNARS

"A FRAMEWORK TO AUTHENTICATE RECORDS IN A GOVERNMENT ACCOUNTING SYSTEM IN BOTSWANA TO SUPPORT THE AUDITING PROCESS"

My name is **Olefhile Mosweu**, a PhD student in the Department of Information Science, University of South Africa (Unisa). My student number is **58553304**. I am conducting an empirical study on "***A framework to authenticate records in a Government Accounting System in Botswana to support the auditing process".*** The study is about the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. The study would also propose a framework for ensuring that authentic reliable records are created and stored in GABS to support auditing processes in the public sector of Botswana.

The findings of the study stand to benefit the Government of Botswana in terms of creating and maintaining authentic reliable digital accounting records for decision making, accountability purposes and meeting the requirements of auditors of financial statements. This is particularly crucial in an era where the Government of Botswana is implementing its e-Government strategy whose services produce digital records. The said records have to conform to appropriate legislation and standards in order to be accepted by auditors as electronic evidence in the audit process.

The confidentiality of study participants will be ensured on the data collected. Participation is voluntary and the study is purely for academic purposes. In order for participants to remain anonymous, names are not required. The interviews are intended to seek opinions on the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. You can call me at +267 72569181/+267 3688 227 or email me at olfmos@gmail.com if you have questions concerning this study. You can also get in touch with my supervisor, Professor Ngoepe, UNISA at ngoepms@Unisa.ac.za if you need further clarity.

Thank you in advance

Yours faithfully

____

Olefhile Mosweu

I hereby give consent for my participation in this study and that the information I give out be ONLY be used for purposes of accomplishing the purpose of this study. Please append your signature to confirm your consent to taking part in the study.

Participant signature: __________ **Date**: ______________

Interview schedule

Objective 1: To analyse the legislative framework for the creation of authentic reliable digital records stored in GABS in support of auditing processes in the public sector of Botswana

1. As the custodian of public records, what role does BNARS play in ensuring public sector records in e-government systems are created and maintained authentic as long as needed?

2. What standards and guidelines are in place to guide and promote the creation and maintenance of authentic digital records? Please explain.

3. Which legislative instruments and policy documents regulate the creation and maintenance of authentic reliable digital records in the public sector of Botswana?

4. To what extent are issues of digital records authenticity over time adequately addressed by available legislation and policies?

Objective 2: To find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

5. Has BNARS 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.

Objective 3: To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS.

6. What level of training/qualifications do you have in records management?

7. What competencies do records management personnel need to declare that digital records (data) created and stored in GABS have their integrity and identity (authenticity) maintained over time?

8. What would be the impact of inadequate ICT competencies and skills for records managers in ascertaining the authenticity of digital records?

Objective 4: To determine how digital records created and stored through GABS are managed authentic and reliable to support auditing processes in the public sector of Botswana.

9. Has BNARS issued records disposal guidelines for the management of digital records in the public sector? Please explain your answer.

10. What digital records management strategies are in place to ensure that public sector digital records are preserved for as long as needed?

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

Appendix 12: Interviews: Auditors

"A FRAMEWORK TO AUTHENTICATE RECORDS IN A GOVERNMENT ACCOUNTING SYSTEM IN BOTSWANA TO SUPPORT THE AUDITING PROCESS"

My name is **Olefhile Mosweu**, a PhD student in the Department of Information Science, University of South Africa (Unisa). My student number is **58553304**. I am conducting an empirical study on "***A framework to authenticate records in a Government Accounting System in Botswana to support the auditing process".*** The study is about the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. The study would also propose a framework for ensuring that authentic reliable records are created and stored in GABS to support auditing processes in the public sector of Botswana.

The findings of the study stand to benefit the Government of Botswana in terms of creating and maintaining authentic reliable digital accounting records for decision making, accountability purposes and meeting the requirements of auditors of financial statements. This is particularly crucial in an era where the Government of Botswana is implementing its e-Government strategy whose services produce digital records. The said records have to conform to appropriate legislation and standards in order to be accepted by auditors as electronic evidence in the audit process.

The confidentiality of study participants will be ensured on the data collected. Participation is voluntary and the study is purely for academic purposes. In order for participants to remain anonymous, names are not required. The interviews are intended to seek opinions on the authentication of digital records in a government accounting system to support auditing processes in the public sector of Botswana. You can call me at +267 72569181/+267 3688 227 or email me at olfmos@gmail.com if you have questions concerning this study. You can also get in touch with my supervisor, Professor Ngoepe, UNISA at ngoepms@Unisa.ac.za if you need further clarity.

Thank you in advance

Yours faithfully

____

Olefhile Mosweu

I hereby give consent for my participation in this study and that the information I give out be ONLY be used for purposes of accomplishing the purpose of this study. Please append your signature to confirm your consent to taking part in the study.

Participant signature: __________ **Date**: ______________

Participant biographical profile (Please tick the appropriate response)

1. **Gender**

a. Male_____________b. Female___________

2. **Age**

a. 20 – 30 years ( )
b. 31 – 40 years ( )
c. 41 – 50 years ( )
d. 51 – 60 years ( )

3. **Educational background**

a. Diploma in Computer Science/Studies ( )

b. Degree Computer Science/Studies ( )

c. Masters' Degree Computer Science/Studies ( )

d. PhD Computer Science/Studies ( )

e. Other: ________________________________ (Please specify)

4. **Work experience**

a. 2 - 6 years ( )

b. 7 - 11 years ( )

c. 12 -16 years ( )

d. 17 – 21 years ( )

e. 22 - 26 years ( )

f. More than 27 years ( )

5. **Job designation**: ____________________________________(Please write in full)

A. Objective 2: To find out procedures in place to maintain the authenticity of digital accounting records created and stored in GABS

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

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

8. Has the authenticity of accounting records in GABS ever been in question during audits? If yes, please explain further.

9. Is there an instance where digital records have been rejected as evidence in the audit process and why?

B. Objective 3: To establish skills and competencies needed by auditors, ICT specialists and records managers to authenticate records created and stored in GABS.

10. What specific technical competencies do Auditors need to authenticate/establish and maintain the authenticity and reliability of digital records created and stored in GABS?

11. What would be the impact of inadequate competencies and skills for Auditors in undertaking an audit in a digital environment (i.e. auditing GABS)?

12. What recommendations can you propose to improve the authentication of digital records in order for them to be accepted by auditors in the audit process?