InterPARES Trust Project Report

Title and code:		Ensuring authenticity and reliability of digital records to support the audit process (AF06)
Document type:		Report
Status:		Final Report
Version:		1
Research domain:		Control
Date submitted:		09 July 2018
Last reviewed:		28 February 2018
Author:		InterPARES Trust Project
Writer(s):		Prof Mpho Ngoepe & Mr Jonathan Mukwevho
Research team:		Prof Mpho Ngoepe, Mr Jonathan Mukwevho, Ms Mangi Mulaudzi, Dr Theunis Bekker, Mr Jannie Ferreira, Mr Paul Mullon, Mr Lesetja Maraba & Dr Mphalane Makhura

Document Control

Version history			
Version	Date	By	Version notes
1	15 Jan 2018	MN	

Table of Contents

Abstract or Executive Summary **4**
Research team **4**
Background and literature **5**
Aims and Objectives/Goals **9**
Methodology **9**
Findings **10**
Conclusions **10**
Products **10**
Annexure A: Framework **10**
References **10**
Appendix A: Legal analysis: ECTA **13**
Appendix B: Framework **17**
Appendix C: Checklist **45**

Executive Summary

The significant role of proper records management in the audit process in both the public and private sectors cannot be over-emphasized. Most of the professions such as auditing, health, finance, human resources and law rely on the strength of records management to perform their duties. For example, records management is increasingly becoming the tool that enables organisations to fulfil the requirements of auditors. Lack of supporting documentation during the audit process is an indication of poor accountability and governance in an organisation leading to disclaimer opinions and increased costs of audit. Therefore, as long as auditing is undertaken, relevant and reliable records will be required as evidence. The widespread use of technology to conduct government activities has resulted in an increased generation of digital records. From the auditing perspective, especially in South Africa, many records managers have lamented of auditors who not always accept digital records as evidence to support the audit queries due to lack of guidelines. The problem is compounded by the fact that the majority of governmental bodies in South Africa present inaccurate and unreliable records as evidence to support the auditing process. It is difficult for governmental bodies to prove the authenticity of digital records to support the audit process. As a result, public sector external auditors do not accept digital records as evidence during the audit cycle. Authentic and reliable electronic records enable organisations to defend their actions, improve decision-making, prove ownership of physical and intellectual assets, and support all business processes; it promotes overseeing service delivery, compliance with legislative framework and standards and facilitates a seamless and effortless audit process.

A project to address the certification of trustworthy digital records to support the audit process in South Africa was registered with InterPARES Team Africa in 2015. The aim of the project was to utilise the Auditor-General South Africa as a case study to develop a framework and checklist (see Annexure A and B) that guide auditors to certify the trustworthiness of digital records that support the audit process. The checklist was tested at a South African Water utility company, Rand Water on 15 November 2017. It is hoped that the framework and checklist will also be utilised by other institutions such as courts and other sectors in South Africa and beyond.

Title: Ensuring authenticity and reliability of digital records to support the audit process

Research team

Lead Researcher(s): Prof Mpho Ngoepe, Mr Jonathan Mukwevho & Ms Mangi Mulaudzi

Project Researchers: Dr Theunis Bekker, Mr Jannie Ferreira, Mr Paul Mullon, Mr Lesetja Maraba 7 Dr Mphalane Makhura

Graduate Research Assistants: Mr Olefhile Mosweu

Background and literature

Most of the professions such as auditing, health, finance, human resources and law rely on the strength of records management to perform their duties. For example, records management is increasingly becoming the tool that enables organisations to fulfil the requirements of auditors. Auditing is an independent assessment whereby auditors test the transactions using records as supporting documentation (Dandago 2009). To be in a position to express an audit conclusion in the positive form, it is necessary for the auditor to obtain sufficient appropriate evidence. Lack of supporting documentation during the audit process is an indication of poor accountability and governance in an organisation which can lead to disclaimer opinions and increased costs of audit (Ngoepe 2012). Therefore, as long as auditing is undertaken, relevant and reliable records will be required as evidence.

The widespread use of technology to conduct government activities has resulted in an increased generation of digital records. This new development brings with it such issues as reliability and authenticity of digital records (Parker 2001:270). A digital record can be considered authentic if it retains all the significant properties upon which its authenticity depends, including reliability, integrity and usability. The international records management standard, ISO 15489 considers an authentic record as one that can be proven to be what it purports to be, have been created or sent by the person purported to have created or sent it, and have been created or sent at the time purported.

Reliability means that the record is capable of standing for the facts to which it attests, while authenticity means that a record is what it claims to be (Lee 2005:3). The authenticity of digital records generated and preserved as evidence of how public representatives executed their mandate is of utmost importance. Authentic and reliable digital records enable organisations to defend their actions, improve decision-making, prove ownership of physical and intellectual assets, and support all business processes; it promotes overseeing service delivery, compliance with legislative framework and standards and facilitates a seamless and effortless audit process (International Council on Archives 2010; Mukwevho & Jacobs 2012:34).

The types of digital records as identified by Duranti (2012) include Computer Stored Records: Contain human statements; if created in the course of business, they are records; e.g. e-mail messages, word processing documents, etc. Used as Substantive Evidence (of its content); Computer Generated Records: Do not contain human statements, but are the output of a computer program designed to process input following a defined algorithm; e.g. server log-in records from Internet service providers, ATM records. Used as Demonstrative Evidence (of the action from which they result) and Computer Stored and Generated: A combination of the two: e.g. a spreadsheet record that has received human input followed by computer processing (the mathematical operations of the spreadsheet program). It can be used both or either way. During the audit process digital records may be presented as evidence by auditees from any of the types as identified by Duranti. However, there is always a challenge as in many countries especially in Africa, some government entities have implemented electronic content management (ECM) while others have enterprise resource planning systems while other generate digital records without the benefit of any system (Ngoepe 2017). As a result, the following scenarios or combination of scenarios are likely to exist in organisations enterprise resource planning (ERP), ECM and informal system (Katuu 2012).

1. **ERP (business systems)**

   Business systems are automated systems that create or manage data about an organisation's activities. They include applications whose primary purpose is to facilitate transactions between an organisational unit and its customers, for example, an e-commerce system, client-relationship management system, purpose-built or customised database, and finance or human resources systems. Business systems typically contain dynamic data that is commonly subject to constant updates (timely) and can be transformed (manipulable), and hold only current data (non-redundant). For the purpose of this document, business systems exclude electronic records management systems. These systems tend to contain "data" as compared to "documents" although they can also be used to store documents. If these systems have a dedicated module or component which has specific ERMS functionality, this module is deemed to be a records management system.

2. **Electronic content management system**

   For purposes of this document, an Enterprise Content Management (ECM) system, Electronic Document and Records Management System (EDRMS) or Electronic Records Management System (ERMS) are used interchangeably as long as they include specific records management functionality. Any system which is designed to store "office-type

documents" in such a way that they are managed according to records management criteria, and can be shown to be unaltered, meets the requirements for an ERMS.

Electronic records management systems contain data that is not dynamically linked to business activity (fixed), cannot be altered (inviolable), and may be non-current (redundant). Electronic records management systems (commonly referred to as EDRMS or ERMS) are those systems specifically designed to manage the maintenance and disposition of records. They maintain the content, context, structure and links between records to enable their accessibility and support their value as evidence. Electronic records management systems are distinguished from business systems for the purpose of this document because their primary function is the management of records.

3. **Informal system**

Any system which does not meet either of the definitions above, in particular the following scenarios, can be considered "informal":

- Electronic documents and records stored on local hard drives outside of records management control;
- Documents and records stored on shared drives;
- Documents and records stored in collaboration environments such as Microsoft SharePoint which have not been specifically configured to include records management functionality and controls;
- Documents and records stored on portable media unless these are classified and managed according to a file plan and strict records controls; and
- An EDMS without the use of records management functionality which allows documents to be stored without formal classification, and allows for editing and amendment of documents.

From the auditing perspective, especially in the global periphery, many records management professionals lament of auditors who not always accept digital records as evidence to support the audit queries due to lack of guidelines (Ngoepe & Ngulube 2014). The problem is compounded by the general poor management of records which results in organisations presenting inaccurate and unreliable records as evidence to support the auditing process. The situation is worse in the digital environment as it is difficult for organisations to prove the authenticity of digital records to support the audit process or to present records as evidence in the court of law. For example, media reports

indicate that the South African government struggled to authenticate the Gupta[1] leaked e-mails. Another situation where the authenticity of cell phone records was questioned is in the case of Oscar Pistorius[2] versus the State of South Africa. Due to situations like the ones mentioned above, public sector external auditors do not accept digital records as evidence during the audit cycle. This is the case in many countries such as Botswana (Mosweu 2012), Ghana (Akotia 1996), sub-Saharan Africa (Nengomash 2013), Kenya (Katuu 2015), Zimbabwe (Chaterera 2016) to mention just a few.

For example, according to Ngoepe (2014) the Auditor-General of South Africa regards the authenticity and reliability of records as key component of any entity' risk management process. For instance, at the moment of transitioning between systems (e.g. when control is being passed to different systems) digital records are at greatest risk of losing their authenticity. Major risk occurs during capturing of metadata as digital records are liable to be altered, to lose their original identity, or to be separated from metadata required to establish their authenticity (Bearman 1997:24). The Australian National Audit Office (2006:18) identifies particularly complex business requirements and a large number of electronic business systems in use as the challenge for governmental bodies in achieving robust records management arrangements in today's digital environment. As a result, the use of such systems create a risk that inaccurate or incomplete information could be

[1] The Guptas is an Indian-born South African business family whose most notable members are the brothers Ajay, Atul and Rajesh. The family's strong ties to South African president Jacob Zuma (2009 - 2019), both personally and through its company Oakbay Investments, have been the subject of extensive international scrutiny and caused much political controversy. The ties have led to widespread claims of corruption, undue influence and of state capture - a term which is used to allege that the government undertakes activities and decisions, decides some high level appointments, and determines control of some state enterprises, for the Gupta family's direct or indirect benefit, or in agreement with the family. A series of explosive e-mails show the extent of the Gupta family's control over cabinet ministers, and state-owned companies and their CEOs and boards. The authenticity of the e-mails has been questioned.

[2] Oscar Pistorius, the 'Blade Runner,' is a South African sprint runner who made history in 2012 as the first amputee to compete in track events at the Olympics. He was later found guilty of murdering his girlfriend on Valentine's Day 2013. Sapa (25 March, 2014 10:48) reports details from the cellphone records as follows:

- Murder accused paralympian Oscar Pistorius made his first call of the morning on which he shot his girlfriend Reeva Steenkamp shortly after 3am, the High Court in Pretoria heard on Tuesday.
- Pistorius's first voice call in the early morning of February 14, 2013 was at 3:19am to a number ending in 2251, which was saved on Pistorius's phone as "Johan Silver Woods", police captain Francois Moller said during Pistorius's murder trial. Johan Stander is the head of security at the Silver Woods estate, where Pistorius shot and killed Steenkamp through the locked door of his toilet, apparently thinking she was an intruder. Moller was being questioned by prosecutor Gerrie Nel.
- At 3.20am the phone was used to make an internet connection. Moller told the court earlier this could include use of social networks like Twitter, Facebook, or WhatsApp.
- At 3.20am Pistorius called 082911, an emergency services number. The call lasted 66 seconds. This was followed by another internet connection, and then a call at 3.21am to a number ending in 6797 -- security at the Silver Woods estate.
- Then, at 3.21am Pistorius called 121, his voice mailbox number. A minute later, Silver Woods' security called Pistorius back. More internet connections followed, and then, at 3.55am, Pistorius called his friend Justin Divaris.
- At 4.01am he called his older brother Carl. Pistorius has been charged with the premeditated murder of Steenkamp and contraventions of the Firearms Control Act. He allegedly fired a shot from a Glock pistol under a table at a Johannesburg restaurant in January 2013.
- On September 30, 2012 he allegedly shot through the open sunroof of a car with his 9mm pistol while driving with friends in Modderfontein.

generated, accessed and used when making decisions, auditing process and service delivery (Australian National Audit Office 2006:18). Possible consequences arising from these risks may include adverse publicity, inefficient business activity and a weakened capacity to prosecute or defend allegations, as well as inability to prove ownership of physical and intellectual property (International Council on Archives 2008:23).

There are two senses in which the term authenticity is used in archival practice. In the more colloquial sense of the word it is a process of establishing that a record is what it is purported to be. In the second, legal and diplomatic, sense an authentication is a specific declaration of authenticity made by a competent officer and consists of a statement or an element, such as a seal, a stamp, or a symbol, added to the record after its completion. In this context a declaration of authenticity only guarantees that a record is authentic at one specific time, when the declaration is made and the authenticating element or entity is affixed (Duranti). At the core of archives and records management is the idea that every record is linked to all the records belonging in the same aggregation by a network of relationships, which finds its expression in the archival bond. The archival bond is *originary*, because it comes into existence when a record is created, *necessary,* because it exists for every record (a document can be considered a record only if and when it acquires an archival bond) and *determined,* because it is qualified by the function the record in the documentary aggregation in which it belongs.

Aims and Objectives/Goals

The general purpose of the study was to investigate the development of a framework to guide auditors in assessing the authenticity of digital records. The specific objectives are to:

- Analyse legal framework for authenticating digital records during the auditing process.
- Assess the criteria that auditors use to judge whether the digital records are authentic and reliable to support audit process.
- Develop a framework and checklist to assess authenticity of digital records.

Methodology

The methodology in this project involved a triangulation of data collection tools such as analysis of documents which include legislation, standards, as well as interviews of public sector auditors and

several discussions with research team members. As a result, a total of 7 meetings were held between 2015 and 2018. Furthermore, the AGSA and some project team members were involved in records management seminars with records management professionals and financial officers of governmental bodies in all nine provinces in South Africa in 2016. Gaps were identified in these meetings, discussions and seminars. Information collected helped to develop a framework and checklist for authenticating digital records. The checklist was tested at the Rand Water on 15 November 2017. As well, the framework and checklist were presented at the ProLISSA conference organized by the University of South Africa in March 2017, at the conference organized by the South African Society of Archivists in Cape Town, July 2017 and the international seminar organised by InterPARES Team Africa in Cape Town, December 2017.

Findings

Findings are presented in terms of the objectives of the project mentioned earlier in this document. With regard to the first objective there is a legislative framework in South Africa that provides evidential weight of digital records similar to paper-based records as long as it meets the stipulated requirements. With regard to the second objective there is no guideline with clear-cut criteria that auditors may use to judge whether the digital records are authentic and reliable to support audit process. Lastly, in relation to the third objective a framework and a checklist to assess authenticity of digital records were developed (See annexure B and annexure C).

Conclusions

In conclusion, the checklist flowing from the framework needs to be piloted with a few more auditees. As well, public auditors should be workshopped on records management processes and how to determine the authenticity of digital records. Alternatively, records management officials should form part of the audit team during the audit cycle.

Products

Annexure A: Legal analysis of ECT ACT
Annexure B: Framework
Annexure C: Checklist

References

Akotia, P. 1996. The management of public sector financial records: the implications for good government. Legon: University of Ghana. Available at: http://www.acarm.org/documents/financial.pdf (Accessed 15 May 2017).

Australian National Audit Office. 2006. Record keeping including the management of electronic records. Available at: http://www.anao.gov.au/uploads/documents/2006-07_Audit_Report_61.pdf (Accessed 10 May 2017).

Bearman, D. 1997. *Moments of Risk: Identifying Threats to Electronic Records*. *Archivaria* 62(1997):16-46.

Chaterera, F. 2016. Managing public records in Zimbabwe: the road to governance, accountability, transparency and effective service delivery. *Journal of the South African Society of Archivists* 49: 116-136.

Dandago, K.L. 2009. (ed). *Advanced accounting theory and practice.* London: Adonis & Abbey.

Duranti, L. 2012. Continuity and transformation in the role of archivist. Paper read at 1st Unisa Archives Lecture, Pretoria (South Africa), 1 November. Available: http://www.unisa.ac.za/Default.asp?Cmd=ViewContent&ContentID=22494 [Accessed 6 November 2012].

Katuu, S. 2015. Managing records in a South African health care institutions – a critical analysis. PhD Thesis, University of South Africa, Pretoria.

Katuu, S. 2012. Electronic content management implementation (ECM) in South Africa. *Records Management Journal* 22(1): 37-56.

International Organisation for Standardisation. 2010. *Draft International Standard ISO/DIS 16175-2: Information and documentation- Principles and Functional Requirements for Records in Electronic Office Environments – part 2: Guidelines and Functional Requirements for Records in Electronic Office Environments*. Geneva.

Lee, B. 2005. *InterPARES 2 Project: domain 2: authenticity, accuracy and reliability: reconciling arts-related and archival literature: discussion paper. University of Windsor.*

Mosweu, O. 2011. Auditing, records inadequacy and the lamentations of the Auditor General in conducting performance audits in the Botswana public service. Paper read at the South African Society of Archivists Conference, Pretoria (South Africa), 14 - 15 July.

Mukwevho, J and 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.

Nengomash, CT. 2013. The past, present and future of records and archives

management in sub-Saharan Africa. *Journal of the South African Society of Archivists* 56: 2-11.

Ngoepe, M. 2017. Archival orthodoxy of post-custodial realities for digital records in South Africa. *Archives & Manuscript* 1(45): 31-44.

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).

Ngoepe, M. 2012. Fostering a framework to embed records management in the auditing process in the public sector in South Africa. PhD Thesis, University of South Africa, Pretoria.

Ngoepe, M and Ngulube, P. 2014. The need for records management in the auditing process in the public sector in South Africa. *African Journal of Library, Archives and Science* 24(2): 135-150.

Parker, EG. 2001. Understanding "Authenticity" in records and information management: analysing practitioner constructs. *The American Archivist*. 64: 270-291.

Appendix A: Legal analysis of ECT Act

INTERPRETATION AND ANALYSIS OF THE ELECTRONIC COMMUNICATION AND TRANSACTION ACT

Dr Mphalane Makhura
&
Prof Mpho Ngoepe

1. INTRODUCTION

The Electronic and Communication Transaction Act (ECTA) was enacted in 2002 to give effect to the electronic commerce. Irrespective of the manner in which a commercial transaction was conducted, a record must be generated. In terms section 1 of the Act, data message which is equivalent to a "record" is defined as a data generated, sent, received or stored by electronic means. Such data includes voice, where the voice is used in an automated transaction; and a stored record. ECTA was therefore crafted to cope with evidential needs in a digital commercial environment.

Based on the above context, documentary evidence therefore refers to evidence that is presented in a form of document irrespective of form or medium hence provision of section 1 of the Act. Such evidence can either be primary or secondary evidence. While primary evidence is the most reliable one, secondary evidence may also be relied upon in the absence of the primary evidence. The ease with which documents are created, duplicated and amended on computers poses serious challenges in determining the originality and authenticity of the document and thereby making the auditing process difficult.

2. INTERPRETATION AND ANALYSIS

2.1. Record

A record refers to recorded information irrespective of form or medium. Instead, section 1 of the Act makes reference to data message which is defined as a data generated, sent, received or stored by electronic means which includes voice, where the voice is used in an automated transaction; and a stored record. The Act also covers issues such as the "best evidence rule" and electronic signatures traditionally part of documentary evidence, admissibility and weight of evidence in digital format.

Comments:

Irrespective of form or medium, a record must reflect final business decision in relation to transaction. It is therefore critical for organizations to ensure that proper control and processes exist with regard to records maturity levels. For example, electronic records management systems must be able to declare a document as a record. While auditors can still rely on documents as secondary evidence, the most reliable source of evidence must be a record.

2.2. Electronic signature

The concept “electronic signature” refers to symbols or other data in a digital format attached to an electronically transmitted document as verification of the creator’s intent to sign the document. Sub-section 13(1) of the Act provides that where the signature of a person is required by law and such law does not specify the type of the signature, the requirement in relation to a data message is met only if an advanced electronic signature is used. Sub-section 3(3)(a-b) of the Act further states that, where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if a method is used to identify the person and to indicate the person's approval of the information communicated; and having regard to all the relevant circumstances at the time the method was used, the method was as reliable and was appropriate for the purposes for which the information was communicated.

Furthermore, sub-section 13(4) of the Act provides that where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved. During the auditing process, the burden of proof is therefore on the Auditors to proof contrary.

Subsection 18(1) of the Act further states that where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message. Furthermore, subsection 18(2) provides that where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information. In conclusion, subsection (3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Comments:

While a document is still open for inputs, a record must reflect a final decision whereby inputs can only be applied through version control. In a manual environment, a signature is an indication of the maturity level of the document to be classified as a record. Electronic signature is a critical tool in an electronic environment to eliminate records from non-records. For governance, Electronic Records Management systems (ERMS) must have a component of electronic signature. This will contribute auditing process.

2.3. Authenticity

The concept “Authenticity” implies that the document is what it appears or alleged to be. Sub-section 14(1)(a-b) of the Act provides that where a law requires information to be presented or retained in its original form, that requirement is met by a data message if the

integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection 2 as reflected below:

- Completeness
- Unaltered

Furthermore, the information must be capable of being displayed or produced to the person to whom it is to be presented. Sub-section 17(1)(a-b) of the Act subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

In terms of sub-section 17(2)(a-b), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for the addition of any endorsement or any immaterial change, which arises in the normal course of communication, storage or display.

Comments:

Incomplete document does not provide a complete picture of the business transaction and therefore is misleading. Apart from incompleteness, once a document is declared a record, it cannot be changed unless via version control. Electronic records management systems must therefore be capable of declaring completeness of records as well as protecting them from alterations. In terms of the Act, it is also a requirement that information must be readily available to auditors. Easy retrieval of information is therefore of critical importance.

3.4. Admissibility and Evidential weight

The general rule is that no evidence may be used to prove the contents of a document except the original document itself (best evidence). Furthermore, the record must reflect what it appears or alleged to be. Section 15(2) of the Act provides that Information in the form of a data message must be given due evidential weight. Section 15(3) further states that in assessing the evidential weight of a data message, regard must be given to the following:

- reliability of the manner in which the data message was generated, stored or communicated;
- the reliability of the manner in which the integrity of the data message was maintained;
- the manner in which its originator was identified; and

- any other relevant factor.

Apart from the above, section 15(4) of the Act further provides that a data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Comments

Originality and authenticity of a record is very critical in good governance. Given the complexity of the electronic environment, it remains a challenge to confirm the two (originality and authenticity). Audit trail and version control must be verified to originality and authenticity of records. In order to create comfort for the auditors, Electronic systems must be capable of audit trail and version control. Over and above, it is worth noting that a certified copy of the record is admissible.

3.5. Retention of records

Records retention is an element of records management policy which is informed by both statutory and operational requirements. Sub-section 16 (a-c) of the Act provides that where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if the following exists:

- the information contained in the data message is accessible so as to be usable for subsequent reference;

- the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

- the origin and destination of that data message and the date and time it was sent or received can be determined.

Comments

For successful auditing process within electronic environment, organisation's approved Records Retention Schedule must be embedded in an Electronic Records Management System.

4. CONCLUSION

Given the speed at which the business is conducted electronically, implementation of ECTA is becoming a long overdue exercise. For successful implementation, organizations must also consider international standards.

Appendix B: Framework

AUDITOR-GENERAL OF SOUTH AFRICA

FRAMEWORK TO GUIDE AUDITORS TO ASSESS AUTHENTICITY OF ELECTRONIC RECORDS TO SUPPORT THE AUDIT PROCESS

Document author	
Document owner	**Tshimangadzo Mulaudzi**
Document reference	**2/12/1/1**
Document classification	**Confidential**
Release date	**After approval**

Document control

This document has been reviewed by:

Reviewer	Date reviewed	Signature
Jonathan Mukwevho	20/09/2017	
Prof. Mpho Ngoepe	20/09/2017	
Dr Shadrack Katuu	20/09/2017	
Dr Mphalane Makhura	20/09/2017	
Paul Mullon	20/09/2017	
Lesetja Maraba	20/09/2017	
Tshimangadzo Mulaudzi	20/09/2017	

Revision history

Version	Author	Date	Revision
V.1	Jonathan Mukwevho	07/06/2016	
V.2	Tshimangadzo Mulaudzi		**2**
V.2.1			
V.2.3			
V.2.4			

Document distribution list

Name	Title
	Auditor-General
	Deputy Auditor-General
	National Leader: Audit Services
	Corporate Executive: Audit
	Business Executive: Audit
	Business Executive: ICT (Chief Information Officer)
	Head of Risk and Ethics
	Senior Manager: Projects – ICT

Document configuration record

Project charter	
Document owner	Tshimangadzo Mulaudzi
Location	Information and Knowledge Management
Item type	Baseline management product
Item attributes	Document
Source	In-house
List of related products (relationship to other documents)	Literature review Annotated bibliography Legal analysis Non-disclosure agreement
Cross references	
Related issues	None
Related risks	None

Table of contents

1 Definitions of acronyms and terms 21
2 Purpose and introduction 25
3 Scope 25
4 Framework for records authenticity 25
5 Assurance 27
6 Governance, risk and compliance 27
7 Records life cycle 29
8 Operational / Internal / Management controls 31
9 Record artefact 34
10 Presentation of audit evidence to auditors 36
11 Generic test scenarios 37
12 Guidelines for applying and interpreting the result of the authentication checklist 39
REFERENCES 42
ANNEXURE B: GUIDELINE FOR SUBSTANTIVE TEST ON THE RECORD ARTEFACT 44

1 Definitions of acronyms and terms

The following are definitions of terms, abbreviations and acronyms used in this document.

Term	Definition
ABU	Audit business unit
AG	Auditor-general
AGSA	Auditor-General of South Africa
AoPO	Audit of predetermined objectives
Application Controls	**IT application controls** are controls that relate to specific computer software applications and the individual transactions. There are typically three types of application controls: input controls (transactions captured, accurately recorded and properly authorised); processing controls (transaction processing has been performed as intended); and output controls (accuracy of processing result).
Archival bond	The **archival bond** is a concept in **archival** theory referring to the relationship that each **archival** record has with the other records produced as part of the same transaction or activity and located within the same grouping.
ARD	Audit, Research and Development
Assurance	As per King IV, **assurance** is the diligent application of mind to evidence, resulting in a statement of declaration concerning an identified subject matter or subject matter information, and which is made for the purpose of enhancing confidence in that subject matter or subject matter information.
Audit process	An assessment of the stewardship of public funds, implementation of government policies and compliance with key legislation in an objective manner.
Authenticity	Refers to the genuineness (not a counterfeit) of a document and absence of tampering, typically inferred from internal and external evidence, including its physical characteristics, structure content and context
Authoritative	Records, regardless of form or structure, which possess the characteristics of

Term	Definition
record	authenticity, reliability, integrity and usability needed to be authoritative evidence of business transactions and fully meet the requirements of the business.
Business process	**A business process** is a collection of linked tasks which find their end in the delivery of a service or product to a client. It is a set of activities and tasks which, once completed, will achieve an organisational goal.
CE	Corporate executive
CIO	Chief information officer
Combined Assurance	Integration, coordination and alignment of **assurance** processes / activities in an organisation to maximise risk and governance oversight and control efficiencies, and to optimise overall **assurance**, considering the organisation's risk appetite. A combined assurance model is applied to provide a coordinated approach to all assurance activities. It aims to optimise the assurance coverage obtained from management, internal assurance providers and external assurance providers on the risk areas affecting the organisation.
DAG	Deputy auditor-general
EDRMS	An electronic document and records management system is a system on which records are collected, organised and categorised to facilitate their secure preservation, retrieval, use and disposal and to ensure that records management standards are met.
Electronic records	Data or information that has been captured and fixed for storage and manipulation in an automated system and which requires the use of the system to render it intelligible by a person.
Evidence	**Evidence** is the available body of facts or information indicating whether a belief or proposition is true or valid.
General IT controls	**IT general controls** are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. These controls apply to mainframe, server and end-user environments.
Governance	Corporate governance, for purposes of King IV, is defined as the exercise of

Term	Definition
(corporate governance)	ethical and effective. leadership by the governing body. It is generally considered to be a hierarchical framework for guidelines, policies, responsibilities and procedures to ensure a certain level of control within an organisation. Although the governance literature proposes several definitions, most rest on three dimensions, namely authority, decision-making and accountability.
GRA	Graduate research assistant
GRC	Governance, risk and compliance
ICT	Information Communication and Technology
IKM	Information and Knowledge Management
Internal / management / process controls	**Internal operational or management control** is a process designed to provide reasonable assurance about the attainment of organisational objectives. Internal control for IT includes the management, operational and technical safeguards prescribed for an information system to protect the confidentiality, integrity and availability of the system and its information. The purpose of internal IT control is to demonstrate reasonable assurance that security risks are kept to an acceptable level.
InterPARES	International research on permanent authentic records on electronic systems: This is a major international research initiative in which archival scholars, computer engineering scholars, national archival institutions and private industry representatives are collaborating to develop the theoretical and methodological knowledge required for the permanent preservation of authentic records created in electronic systems.
ISA	Information System Audit
NARSSA	National Archives and Records Services of South Africa Act, 1996
Preservation	**Preservation** refers to the processes and activities that stabilise and protect objects so that they will be permanent and durable or as long lasting as it is possible to make them (authors).
QC	Quality Control
RE	Risk and Ethics

Term	Definition
Record	The record is the final statement about the transaction or business process which it represents. Once "declared", it remains unaltered over, no matter how many times it is recalled for use. It will contain unique information and/or data and is likely to be the end result of a document and version management process.
Record storage	Providing a reliable storage location to protect the integrity of records and to ensure that they are not altered or tampered with.
Reliability	The degree to which the record is dependable, consistent and worthy of trust.
Risk and risk management	**Risk** is the potential that a given threat will exploit vulnerabilities of an asset, or group of assets, to cause loss or damage to the asset. According to ISO 31000, risk is the "effect of uncertainty on objectives" and an effect is a positive or negative deviation from what is expected. The following two paragraphs will explain what this means. **Risk management** is the process to identify and assess risk and to apply methods to reduce it to an acceptable level. It aims to identify, measure and control uncertain events and to assist organisations to better manage risks associated with their missions.
SBU	Support business unit
Structured records	Structured records are records that are kept in a structured form in columns and rows in a database.
Substantive procedure (Test)	**Substantive procedures (or substantive tests)** are those activities performed by the assurance provider to detect material misstatement or fraud at the assertion level. It is a process, step or test that creates conclusive evidence regarding the completeness, existence, disclosure, rights or valuation (the five audit assertions) of assets and/or accounts in the financial statements. It assists in documenting sufficient evidence to provide reasonable assurance for the assurance provider's conclusions.
Unstructured system	Unstructured records are those recorded objects that are not kept in rows and columns in a database, like text-based or visually rich records (audio, video, etc.).

2 Purpose and introduction

The purpose of this document is to provide guidelines for auditees to present authentic records to support the auditing process. The document outlines the conditions necessary to ensure reliability and authenticity of records.

There are two senses in which the term authenticity is used in archival practice. In the more colloquial sense of the word it is a process of establishing that a record is what it is purported to be. In the second (legal and diplomatic) sense an authentication is a specific declaration of authenticity made by a competent officer and consists of a statement or an element, such as a seal, a stamp or a symbol, added to the record after its completion. In this context a declaration of authenticity only guarantees that a record is authentic at one specific time, when the declaration is made and when the authenticating element or entity is affixed.

3 Scope

The scope of the framework is limited to electronic or digital records generated on the various systems deployed by the organisation to enable and execute its business processes in order to fulfil its regulatory obligations. These could be either business systems or record management systems. The project is limited to regularity audits. Therefore, other types of audits, such as forensic audits, are not included in the scope. The associated information / IT systems audit is not discussed in detail in this framework, but form an integral part of the framework, especially in terms of the reliance that can be placed on general IT controls and application controls. The audit does not focus on records management as a discipline, but rather on electronic records in the context of a business process. However, record management controls across the life cycle of the record impacts the authenticity of electronic records.

4 Framework for records authenticity

4.1 Overview

The framework identifies the various elements that need to be considered during the audit process. Each of these elements has the potential to directly or indirectly impact on the authenticity of electronic records, which may be used as evidence during the audit. While the focus is on a regularity audit, the same principles could be adopted in any form of audit. The emphasis is on the auditee's electronic records and associated IT systems. However, the auditors should ensure that their own records generated during the audit process are

evaluated for authenticity using the same principles. Any record received, captured, stored and used during the audit process should be similarly evaluated.

4.2 Evidence

Evidence is the available body of facts or information indicating whether a belief or proposition is true or valid. Records provide evidence of business processes. They document what people do as public servants of any governmental department or entity and can be in any format. Evidence includes all electronic records produced for inspection of auditors or courts of law. As a rule, nothing should apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record. Detailed explanation regarding what constitutes audit evidence in an audit of financial statements, in compliance with applicable standards, legal and regulatory requirements is discussed in **section 10** of this document.

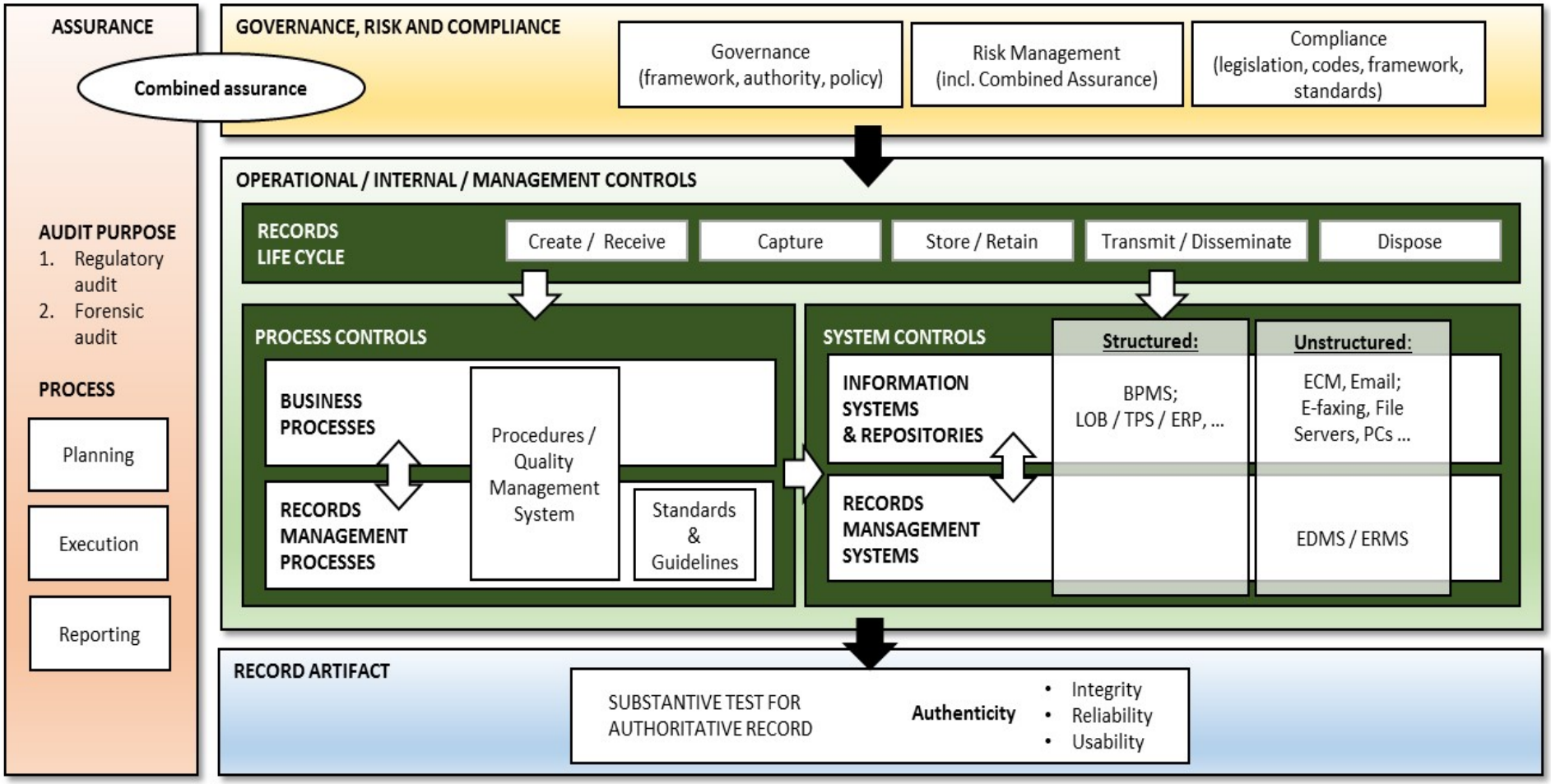


Figure 1: Framework diagram

5 Assurance

The audit process is an assessment of the stewardship of public funds, implementation of policies and compliance with key legislation in an objective manner. It helps governmental bodies achieve their objectives by following a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

An audit process includes preliminary engagement activities, overall audit strategy, detailed planning and execution, concluding, reporting and quality control. Auditors meet the heads of business units or sections or senior managers within the public institution during audit process where records are requested or made available. Asset-related records such as asset registers, audit of predetermined information such as a strategic plan, supporting document of achievements, and human resource records such as leave files, minutes of meetings of the selection committee, and supply chain management records such as payment batches and tender documents are made available. The above process is followed when the AGSA conducts its annual regularity audit.

Regularity auditing comprises financial auditing, auditing performance information and testing of compliance with legislation. The audit approach followed by the AGSA is a combination of a risk-based and a transaction cycle approach. This framework focuses on regularity audit and business processes that are inspected during the audit process.

6 Governance, risk and compliance

The audit and determination of authenticity takes place within the context of the institutional regulatory environment or the organisation's integrated governance, risk and compliance environment.

6.1 Governance

Governance includes corporate governance, Information Technology (aka Digital Technology or Information & Communication Technology) governance and information governance.

Corporate governance includes, but is not limited to, the various policies and the decision-making authority that govern business processes and the electronic records within the context of that business process. One of the key aspects of corporate governance in relation to electronic record authenticity is the decision-making authority (e.g. governance framework and / or delegation of authority matrix) that determines the authority to make key decisions, including the approval of the associated records and/or process steps. The decision-making authority translates into operational business process controls or procedures. The policies further determine the extent to which records can be used electronically, and provide the basis for electronic signatures.

IT governance, or the corporate governance of ICT, is addressed by King III for corporates and the Department of Public Service and Administrations' Corporate Governance of ICT Policy Framework (DPSA CGICTPF) for the South African Government. It is part of, and must be integrated with, corporate governance, but it focuses on IT / ICT / Digital Technology. In relation to the authenticity of electronic records, it includes the required directives or policies associated with system controls, especially general IT controls (e.g. security / access control; manage change). The governance of technology and information is addressed and defined by King IV. Even though the governance of information was included in IT governance, as defined by King III, the King IV code now places more emphasis of the governance of information independent of the media (i.e. data, records, knowledge), or all intellectual capital of the organisation. This includes the directives or policies associated with the management of electronic records, whether part a formalised system (i.e. ERP data), or an informal system.

6.2 Compliance

Compliance includes the laws and regulations within which the entity operates. This includes codes of practice, industry regulations and standards that govern the industry sector. The Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) (ECT Act) and National Archives and Records Service Act, 1996 (Act No. 43 of 1996) provide essential context when determining whether records can be managed electronically. The National Archives and Records Services of South Africa Act gives the National Archivist the responsibility to determine and prescribe the conditions with which electronic records systems must comply, while the ECT Act awards electronic records a status similar to paper-based records to be legally admissible, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any doubt. These are supported by various standards which provide guidance on how to manage electronic records. Compliance also includes regulations directly related to the business processes being audited and therefore the necessity for, and approval of, records associated with that business process (e.g. National Treasury directives relating to supply chain management). Compliance to codes, such as King IV or the DPSA CGICTPF, for IT / Information governance is also important, if relevant.

6.3 Risk management

Risk-based assurance, as included in the combined assurance discipline, includes placing the emphasis of assurance efforts on controls and levels of defence (i.e. level 1: management of risk / risk owner and level 2: management support and oversight) relating to higher risks areas. This relates indirectly to the prioritisation of the assurance efforts based on the risk associated with the business process and the electronic records relating to the business process. The risk associated with the business process being audited also impacts the decision or necessity to perform substantive tests

related to the authenticity of electronic records, whether reliance can be placed in the system controls (i.e. general IT controls and application controls), or not.

7 Records life cycle

The authenticity of electronic records must be maintained across its full life cycle, from its creation to disposal stage, in order to provide assurance that it has not been altered in any unauthorised or undocumented manner.

7.1 Creation / receipt

The responsibility to create records that document regular business transactions involved providing evidence of the department decisions or actions. It is therefore important to create records within the public institution for evidentiary, transparency and accountability purposes. Such records should be saved or filed along with the others that support the same task. Record creation includes processes whereby records are converted from one format to another, most often through the process of scanning or digitising from paper to an electronic image. The process by which these records are converted should be analysed to ascertain whether the records could have been manipulated during the process. The main methods for creating and retrieving digital records as authentic include profiling records and retrieving records in context. A list of fields included in the record profile form is discussed in the record profiling section of this document. A checklist for assessing authenticity of electronic records during the audit process at this stage is attached as ***appendix A.***

7.2 Capture

The capture activity includes those steps that are taken to formally enter the record into the records system, with any forms of identification, classification, indexing or other metadata being created and formally linked or associated with the record. It also includes identifying business information as records and putting them aside for future use and reference, registering a record by assigning it a unique identifier and entering, generating or copying metadata into a record profile. Metadata is one of the key tools for the capture and control of official records. It is essential for the purpose of searching and finding specific individual records or groups of records.

7.3 Storage and retention

The third stage, storage and retention, is the portion of the records life cycle where the record is either stored at the department while in active use, or is maintained remotely when use is less frequent, thus

providing a reliable storage location and ensuring that records are not altered or tampered with to protect their integrity. Storage and retention include the preservation of records identified as having lasting value, often exceeding the time for which records have value to the organisation. The record must be kept in such a manner that it remains accessible and usable for the period for which it is required, which may include permanent preservation.

The department may need to retain the record for a period of time longer than the life of the electronic information system that generated the electronic record or electronic signature, which poses special challenges insofar as maintaining the trustworthiness of the record when migrating from one system to another. For a record to remain reliable, authentic, with its integrity maintained, and usable for as long as the record is needed, it is necessary to preserve its content, context and sometimes its structure.

A trustworthy record preserves the actual content of the record itself and information that relates to the context in which the record was created and used. Specific contextual information will vary depending on the business, legal and regulatory requirements of the activity to which the record relates. It also may be necessary to preserve the structure or arrangement of its parts. Failure to preserve the structure of the record will impair its structural integrity, which in turn may undermine the record's reliability and authenticity. It therefore becomes important for archivists to ensure the authenticity, reliability and long-term accessibility of permanent electronic records for current and subsequent users.

Protecting the authenticity of the electronic record involves performing several activities, such as establishing security and access controls (i.e. general IT controls), ensuring the integrity of the record, managing metadata, managing storage media, managing the content of digital objects, and planning for emergencies. These activities are important regardless of whether a formal preservation programme has been established. In other words, even if the organisation has not decided to establish specific preservation procedures (e.g. refreshing, replication, emulation or migration), it can take steps to improve the probability that digital object will be protected. The main methods for creating and retrieving digital records as authentic include profiling records and retrieving records in context.

7.4 Transmission and dissemination

Records are often transmitted to and shared with other parties, either during or after the business process. Metadata reflecting the movement of all records should be kept, as this may provide insight into who conducted any actions on the record. A clear distinction should be made between the record used for auditing, and any copies which may have been created and which are not deemed to be the record.

7.5 Disposal

Disposal includes the destruction of records, archiving or records and transferring records to an archive repository. Archiving and transfer do not form part of the business process, but these may be audited to determine whether sound record management processes are being followed. An audit of the business process should include analysis and determination of whether electronic records are destroyed/deleted as a part of the business process. This could include destruction of a physical record after scanning, in which case the processes should be carefully scrutinised to determine whether the resulting images are authentic and reliable as evidence.

8 Operational / Internal / Management controls

A presumption of authenticity can be derived if the appropriate general IT controls (e.g. access control, change management), application controls and process controls are in place and are effectively applied. This requires that at least the following attributes are intact:

- Ability to identify the records, the persons involved in their processing, any action or activity carried out on the records, dates of transmissions, contextual and classification links to a file plan, and any associated or attached documents;
- Access privileges are identifiable, intact and effectively maintained and controlled;
- Protection mechanisms are in place to prevent alteration, loss, corruption or destruction of records;
- Documentary forms of records are identified for each process; and
- Authentication and approval mechanisms are documented.

8.1 Process controls

A business process is a collection of linked tasks which find their end in the delivery of a service or product to a customer or stakeholder. It is a set of activities and tasks which, once completed, will accomplish an organisational goal. Governmental institutions in the regular course of business or activity create or receive, maintain, use and dispose of any memorandum, writing, entry, representation or combination thereof of any act, transaction, occurrence or event. Transactions may involve the transfer of funds in terms of value, and transactions where the information generated may later be subject to audit or compliance in terms of information requirements. During the regular course of business, conditions should allow for the production, accurate reproduction and maintenance of authentic and reliable electronic records that can be admissible as evidence. At any stage in a business process information may be created, received, captured, used or stored in the normal course of business. Process controls translate into application controls, as enforced by the relevant IT system(s) enabling the business process.

For the purpose of this framework, a distinction is made between a business process and a records process. The latter is a separate process carried out by records staff to manage records under their control that had been received from the business units. Records processes include:

- classification against a file plan or other classification scheme
- allocation of metadata other than that created during the business process
- storage activities once the record is under the control of the records management system
- development and application of retention periods
- preservation activities to ensure usability of the record into the future
- disposal in terms of retention schedules and disposal authorities
- transfer to archival institutions.

8.2 System controls

8.2.1 Information and records management systems

Governmental bodies' information and records management system is a corporate area of endeavour involving the administration of all business records from creation to disposal stage. Information and records created or received within the organisation may be stored and managed in both electronic systems and paper-based systems. Electronic systems may include electronic document management systems, electronic records management systems and business systems such as ERP systems. A paper-based system may include printed business-related emails; however, it does not form part of this framework. Sound records management principles should be applied to business and electronic document and record systems, which in this document have been categorised into structured and unstructured systems.

IT / Information system and repositories, which manage transactions and functional areas of the business, are generally not dedicated to records storage, but often contain varying degrees of records management functionality.

An **electronic records management system** is often implemented as part of broader suite of products known as an Electronic Document and Records Management System (EDRMS), or Enterprise Content Management (ECM) system. National Archives (NARSSA) stipulates that all government bodies must implement an EDRMS capable of managing electronic records according to their requirements. The functionality required by NARSSA should be present, regardless of whether this is:

- a standalone system
- part of an EDRMS suite
- part of an ECM suite

- part of the ERP or line of business system.

8.2.2 Structured vs unstructured

Structured systems are typically line of business systems, such as ERP systems, and email systems that are transaction-based and focus on structured data, rather than unstructured data (documents or records or images). They may, however, provide functionality that allows for records to be stored. This functionality may allow a scanned image, born-digital document or email attachment to be saved in such a way that it is linked to the transaction. In some cases, a dedicated records module is provided as part of the overall functionality. Structured systems are normally managed in a more formal way according to database management principles and procedures. The National Archives and Records Services Act requires that they be managed in such a manner that the authenticity and reliability of the records contained in those systems can be proven beyond any doubt. The information contained in these systems also constitute public records that form part of the corporate memory of governmental bodies and therefore need to be managed according to the same principles by which all other records are managed. However, this system must utilise security measures to ensure their integrity.

Unstructured records refer to records that are not kept in the governmental body's formal record-keeping systems, such as email, records created on individual PCs' hard drives, records stored in shared network drives or file servers, etc. Whereas it is necessary to manage records in structured systems, it is even more important to have proper systems to manage records in unstructured systems for the simple reason that unstructured records can very easily be forgotten and not be managed according to sound records management principles, thus compromising their integrity and legal admissibility. Records residing in unstructured systems should be maintained and retrieved in a manner which ensures that they retain their authenticity and reliability as evidence of transactions. The most sensible way to do this is to use an electronic records management application. The purpose of an electronic records management application is to manage all unstructured electronic records within an organisation, including scanned images, Word documents, email, web-based activities, etc. These systems have an added benefit in that they also manage records in other formats to ensure that all records are managed in an integrated manner.

This framework focuses on electronic documents and records, together with their meta data, from creation to disposal phase, and made available by governmental bodies to auditors during regularity audit.

8.2.3 General IT and application controls

General IT and application controls are key elements of the organisation's collection of internal / operational or management controls. These are applicable to, and required for all information

systems that store or manage electronic records relating to the business process being audited. Examples of typical general IT and application controls focused on when determining whether reliance can be placed on them are: 1) IT / information / cyber security (e.g. access control, segregation of duties, audit trails, etc.); 2) physical security measures relating to ICT assets; and 3) managing change to the IT system (i.e. change control to avoid uncontrolled changes). The emphasis is placed on operational and technical safeguards prescribed for the information system to protect the confidentiality, integrity and availability of the system and its information, such as electronic records.

> *The authoritativeness of records is supported by their being managed by records systems that are reliable, secure, compliant, comprehensive and systematic" [ISO 15489:2016: Information and documentation – Records management Part 1: Concepts and principles].*

9 Record artefact

When reliance cannot be placed on the general IT / system controls, no presumption of authenticity can be derived. The assurance provider may need to conduct substantive tests, or more substantive tests, of transactions, business activities or the associated electronic records. In relation to the authenticity of electronic records in the context of a business process, it means auditing the authenticity of the record based on the characteristics (including meta data), context, content and structure of the electronic record itself. In such a situation, all tests for record authenticity should check whether the records meet the criteria of an authoritative record as per ISO 15489:2016: Information and documentation – Records management part 1: Concepts and principles.

> *Records are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which is used, received or produced in the course of business activity.*
>
> *While a record is usually evidence of a single transaction, in some cases a sequence of records may be needed to represent a given transaction. Records may exist individually, or may form aggregations that have been designed to document business processes, activities or functions.*
>
> *Records, regardless of form or structure, should possess the characteristics of authenticity, reliability, integrity and usability to be authoritative evidence of business transactions and fully meet the requirements of the business.*

9.1 Record profile

A record profile is an electronic form that is generated when a digital record is either made or received or, in the case of paper-based records, when it is forwarded to the central records system.

The purpose of a record profile is to identify a record in a unique manner and to place it in relation to other records belonging in the same aggregation. Below is a list of fields included in the record profile form:

Field	Description
Protocol number	This is the sequential number assigned to each incoming or outgoing record in the protocol register. In the case of paper-based records, this is the item number. Irrespective of the number of pages, it is assigned one number. There is also a protocol number of the sending office. This also applies to scanned records. NB. The auditors can be shown the protocol number in an electronic system or in an ERP.
Date of receipt (date stamp)	The date the record is received by the organisation to which it was sent. The date must correspond with the date on which the record is assigned a protocol number.
Time of receipt	The time when the record is received by the organisation to which it was sent. This element is not relevant to paper-based records.
Date of transmission	The date on which the record leaves the space in which it was generated, either from one space to another or from the general space to outside the organisation, or from the records office to outside the organisation. Digital records will have a time of transmission.
Date of record	The date assigned to a record by the author.
Archival date	The date assigned to a record by the record office, i.e. the date that appears on the date stamp.
Author's name	The name of a person competent to issue the record or in whose name or by whose command the record has been created.
Medium	The physical carrier of a record.
Number of attachments	

Table 1: Record profile fields

9.2 Archival bond

The main methods for creating and retrieving digital records as authentic include profiling records and retrieving records in context. At the core of archives and records management is the idea that every record is linked to all the records belonging in the same aggregation by a network of relationships, which finds expression in the archival bond.

The archival bond is:

- originary, because it comes into existence when a record is created
- necessary, because it exists for every record (a document can be considered a record only if and when it acquires an archival bond)
- determined, because it is qualified by the function of the record in the documentary aggregation in which it belongs.

This involves identifying a set of electronic information to serve as the evidential record, comprising both content and context. In order for information to have the capability of functioning as a record, it is necessary to augment that content information with additional data (that is, metadata) that places it in the context of the business operations and computing environment in which it was created.

10 Presentation of audit evidence to auditors

Following on from section 4.2 of this framework, section 14(1) of Public Audit Act, 2004 (PAA) requires auditees to submit any document, book or written or electronic record or information which reflects or may elucidate the business, financial results, financial position or performance which are subject to the Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA), as amended, or the Municipal Finance Management Act, 2003 (Act No. 56 of 2003) (MFMA). Among other things, such audit documentation must meet the requirements of International Standard of Auditing 230 (ISA 230) and the specific documentation requirements of other relevant ISAs to provide evidence of the auditor's basis for a conclusion about the achievement of the overall objectives of the auditee; and evidence that the audit was planned and performed in accordance with ISAs and applicable legal and regulatory requirements.

ISA 500 explains what constitutes audit evidence in an audit of financial statements, and deals with the auditor's responsibility to design and perform audit procedures to obtain **sufficient, relevant and reliable audit evidence** to be able to draw reasonable conclusions on which to base the auditor's opinion. For instance, ISA 500 stipulates that original documents are more reliable than photocopies or facsimiles and digitised records, and that reliability depends on the control over their preparation and maintenance. Whereas ISAE 3000 notes that an audit process rarely involves the authentication of records and does not require the auditor to be trained or be an expert in determining authenticity of records, ISA 240 states that conditions identified during the audit process will merely cause the auditor to believe or not believe that supporting documentation is authentic. However, none of the

abovementioned standards provide the criteria which the auditor may use to assess authenticity of electronic records made available.

The Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) states that electronic records enjoy the status as paper-based records in determining whether they are legally admissible, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any doubt. In other words, the above act provides for the environment (the 'what') conducive to assessing the authenticity and reliability of electronic records, but not the "how". To this end, the National Archives and Records Service's issued two documents – [3]*Managing electronic records in governmental bodies: Policy, principles and requirements* and [4] *Managing electronic records in governmental bodies: Metadata requirements also provide guidance for public institutions in managing records generated in an electronic environment.* In addition, ISO 15801: 2017[5] *Document management -- Electronically stored information -- Recommendations for trustworthiness and reliability* can be used to demonstrate that, once the electronic information or records is stored, output from the system will be a true and accurate reproduction of the electronically stored information created and/or imported. However, it does not cover processes used to determine whether electronically stored information can be considered to be trustworthy prior to it being stored or imported into the system. These standards and guidelines provide the foundation to further develop the framework and checklist to assess the trustworthiness of records used in audit processes conducted by the AGSA. Simply put, the checklist could provide guidance to auditors during the substantive tests when determining whether an electronic record can be presumed to be authentic and reliable based on the characteristics, structure, content and context of the record artefact. It is imperative to start by providing generic test scenarios that are likely to exist in the organisation/departments/auditees, followed by guidelines on the interpretation of the checklist ***(See annexure A).***

11 Generic test scenarios

The following scenarios or combination of scenarios are likely to exist in organisations.

(Source: Most of the definitions have been extracted and amended from ISO 16175-2 – Principles and functional requirements for records in electronic office environments.)

A - ERP (business systems)

[3] https://www.nationalarchives.gov.za/sites/default/files/Managing_electronic_records_Policy__principles_and_Requirements_April_2006.pdf

[4] https://www.nationalarchives.gov.za/sites/default/files/Managing_electronic_records_metadata_requirements%20April%202006.pdf pp 13-22

[5] https://www.iso.org/standard/66856.html

Business systems are automated systems that create or manage data about an organisation's activities (for the purpose of this document). They include applications whose primary purpose is to facilitate transactions between an organisational unit and its customers, for example, an e-commerce system, client-relationship management system, purpose-built or customised database, and finance or human resources systems. Business systems typically contain dynamic data that is commonly subject to constant updates (timely) and can be transformed (manipulable), and hold only current data (non-redundant). For the purpose of this document, business systems exclude electronic records management systems. These systems tend to contain "data" as compared to "documents" although they can also be used to store documents. If these systems have a dedicated module or component which has specific ERMS functionality, this module is deemed to be a records management system.

B - Electronic records management system

Electronic records management systems contain data that is not dynamically linked to business activity (fixed), cannot be altered (inviolable), and may be non-current (redundant). Electronic records management systems (commonly referred to as EDRMS or ERMS) are those systems specifically designed to manage the maintenance and disposition of records. They maintain the content, context, structure and links between records to enable their accessibility and support their value as evidence. Electronic records management systems are distinguished from business systems for the purpose of this document because their primary function is the management of records. For purposes of this document, an Enterprise Content Management (ECM) system, Electronic Document and Records Management System (EDRMS) or Electronic Records Management System (ERMS) are used interchangeably as long as they include specific records management functionality. Any system which is designed to store "office-type documents" in such a way that they are managed according to records management criteria, and can be shown to be unaltered, meets the requirements for an ERMS.

C - Informal system.

Any system which does not meet either of the definitions above, in particular the following scenarios, can be considered "informal":

- Electronic documents stored on local hard drives outside of records management control
- Documents stored on shared drives
- Documents stored in collaboration environments such as Microsoft SharePoint which have not been specifically configured to include records management functionality and controls
- Documents stored on portable media unless these are classified and managed according to a file plan and strict records controls
- An EDMS without the use of records management functionality which allows documents to be stored without formal classification, and allows for editing and amendment of documents.

12 Guidelines for applying and interpreting the result of the authentication checklist

The checklists for assessing the authenticity and reliability of electronic records in each records phase (i.e. creation / approval / capturing and records storage and preservation / archiving) during the audit process are attached to this document *(see annexure A).* The checklist consists of focus areas such as business process, records management information, IT general controls, application controls and substantive test of record artefact in terms of this framework. Each area is further subdivided into requirements, accompanied by assessment details or key questions. The assessment can be done against the existing information and records system-generating records which can be used as evidence during audit process. Such systems include EDRMS, ERP or any informal systems:

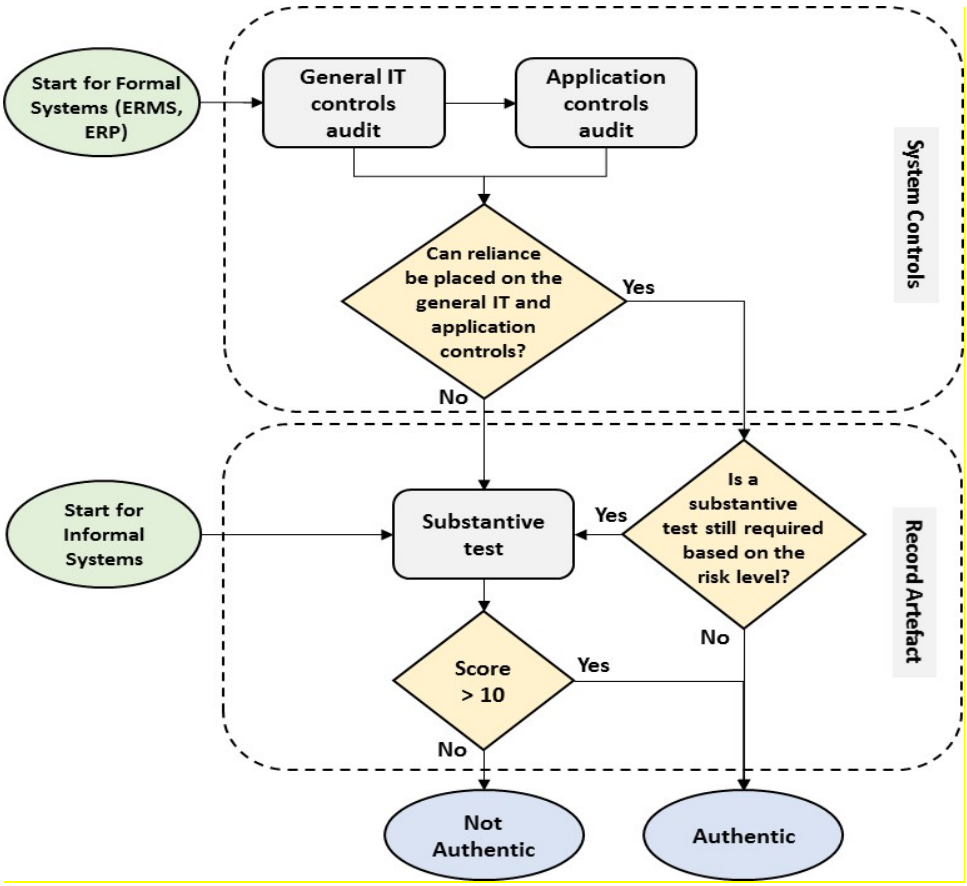
System category	Explanations
EDRMS	Reliance can be placed on the general IT / system controls in that a presumption of authenticity can be derived. The assurance provider might not need to conduct substantive tests or more substantive tests of transactions or business activities, depending on the associated level of risk.
ERP	Reliance can be placed on the general IT / system controls in that presumption of authenticity can be derived. The assurance provider might not need to conduct substantive tests or more substantive tests of transactions or business activities, depending on the associated level of risk.
Informal systems	Reliance cannot be placed on the general IT / system controls in that presumption of authenticity cannot be derived. The assurance provider might need to conduct substantive tests or more substantive tests of transactions or business activities. In relation to electronic records authenticity in the context of a business process, it means auditing the authenticity of the record based on the characteristics (including meta data), context, content and structure of the electronic record itself. In such a situation, all tests for record authenticity should check whether the records meet the criteria of an authoritative record as per ISO 15489: 2016: *Information and documentation – Records management part 1: Concepts and principles.*

13 A basic decision tree for getting to a conclusion

- It is important to first determine whether the information systems auditor performed an IT general control review during the audit. In that regard, the regularity auditor may request ISA during the pre-planning stage of the audit process to include the EDRMS, ERP or other informal system in

their scope for the IT general control review. The outcome of this evaluation may then be used to provide a score for the IT general control environment.

- In the case of a formal system, whether an EDRMS or ERP, the starting point is the audit of the system controls, including general IT controls and application controls, to determine whether or not reliance can be placed on the system controls.
- In the case of an informal system, it is assumed that reliance cannot be placed on the system controls, and such an audit is therefore not required. In such a case, a substantive test must be performed.
- If reliance cannot be placed on the system controls related to an ERDMS or ERP, a substantive test must be performed focusing on the record artefact itself.
- If reliance can be placed on the system controls related to an ERDMS or ERP, the auditor must decide if a substantive test is still required, even if on a smaller scale, depending on the level of risk associated with the business process or process control.
- If a substantive test is not required for a formal system (ERDMS or ERP), the auditor may assume that the evidence derived from that system is authentic and reliable as a fact and enough to make a judgement to reach a sound conclusion. The presumption is therefore made that the record is deemed to be authentic.
- If a substantive test is required, the decision regarding the authenticity of the record is based on a scoring system (i.e. if the score is higher than 10, the record is deemed to be authentic; if the score is 10 or lower, then the record is deemed not to be authentic).


Start for Formal Systems (ERMS, ERP)
General IT controls audit
Application controls audit
System Controls
Can reliance be placed on the general IT and application controls?
Yes
No
Start for Informal Systems
Substantive test
Yes
Is a substantive test still required based on the risk level?
Record Artefact
No
Score > 10
Yes
No
Not Authentic
Authentic

References

1. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002). https://www.acts.co.za/electronic-communications-and-transactions-act 2002/2_objects_of_act (Accessed 22 October 2017).
2. Managing electronic records in governmental bodies: Policy, principles and requirements. https://www.nationalarchives.gov.za/sites/default/files/Managing_electronic_records_Policy__principles_and_Requirements_April_2006.pdf (Accessed 22 October 2017).
3. Managing electronic records in governmental bodies: Metadata requirements. https://www.nationalarchives.gov.za/sites/default/files/Managing_electronic_records_metadata_requirements%20April%202006.pdf (Accessed 22 October 2017).
4. SANS 15801:2013 (Ed. 2.00): Document management - Information stored electronically - Recommendations for trustworthiness and reliability. https://store.sabs.co.za/pdfpreview.php?hash=5749327a14cae7d1caff9612d644e102eb2ccff3&preview=yes (Accessed 22 October 2017)
5. SANS 16175-2:2014 (Ed. 1.00: Information and documentation - Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems. https://store.sabs.co.za/pdfpreview.php?hash=b83213b4b9ab64ad9498da542b87322dde947c0c&preview=yes (Accessed 22 October 2017).
6. ISO 15489:2016: Information and documentation – Records management Part 1: Concepts and principles.
7. ISO/TR 15801:2017: Document management -- Electronically stored information -- Recommendations for trustworthiness and reliability. https://www.iso.org/standard/66856.html (Accessed 22 October 2017).
8. Republic of South Africa. 1999. Public Finance Management Act, 1999 (Act No. 1 of 1999) (PFMA), as amended
9. Republic of South Africa. 2003. Municipal Finance Management Act, 2003 (Act No. 56 of 2003) (MFMA).
10. International Standard on Auditing 230: Audit Documentation. 2009. http://www.ifac.org/system/files/downloads/a011-2010-iaasb-handbook-isa-230.pdf (Accessed 22 October 2017).

11. International Standard on Auditing 500: Audit Evidence, 2009. http://www.ifac.org/system/files/downloads/a022-2010-iaasb-handbook-isa-500.pdf (Accessed 22 October 2017).

12. Republic of South Africa. 2004. Public Audit Act, 2004

13. Katuu, SA. 2017. Assessing records trustworthiness for audit purposes. Unpublished.

GUIDELINE FOR SUBSTANTIVE TEST ON THE RECORD ARTEFACT

For auditors to conduct a substantive test on the record artefact provided during the audit process, the following requirements need to be taken into consideration:

- Ability to prove who and by when the information was created.
- Ability to identify or prevent unauthorised changes to the information.
- When accessing a record, being able to access all relevant parts thereof.
- Establish that the template used is dated.
- When someone is in acting position, be able to establish if there is a scanned letter confirming that.
- Recognise consistency for completed information.
- Establish if there is a control regarding signatures.
- Establish if there is a process in place regulating externally generated records.
- The National Archives and Records Service metadata requirements require the following metadata elements: particular identity, context, relationships, date information, version control, access control, disposal control, record type, presentation and medium, location information, system information, vital record information, and audit information.

NB: It is important that auditors use their judgement regarding the authenticity and reliability of electronic records after conducting the substantive test of record artefact.

Municipality/Department/Entities:	
Date:	
Year end:	
Purpose:	To assess the authenticity and reliability of the electronic records to support audit process
Assessed by:	
Assessment recommendations:	
Reviewed by:	
Date of next review:	

			EDRMS	
Section	**Requirement**	**Assessment details**	**Yes**	**No**
Business Process	Form overlays and form removal			
			0	**0**

			EDRMS	
Section	**Requirement**	**Assessment details**	**Yes**	**No**
Reocrds process/Information		Does the institution rely on information from this system as evidence?		
		Do the records have disposal coverage?		
		Minimum retention specified?		
		Legislative requirements		
		Business requirements		
			0	**0**

			EDRMS	
Section	**Requirement**	**Assessment details**	**Yes**	**No**
IT general controls	Information Management Policy	A Policy Document should be created, then approved by senior management of the organization, and should be reviewed at regular intervals.		
		Must be developed in conjunction with legal advice.		
		Create policy document with detail regarding contents,		

		include access, retention periods and security)		
		The Policy Document should contain details of policy on the storage of versions of documents		
		Individual or job function responsibilities for the Policy Document should be defined . Individual or job function responsibilities for each information type should be identified		
	Retention Schedule	Procedures for the destruction or disposal of information at the end of the retention period should be documented. No source documents should be destroyed until the images have been successfully written to storage and appropriate backup procedures have been completed.		
	Information Security Policy	Implement an Information Security Policy		
		The organization should adopt an Information Security Policy, covering all elements of the information management system. These security measures need to be aligned to any information classification categories that are used.		
		Security measures need to include backup and other copies of stored information, as their integrity is of importance in circumstances where they have been used as replacements for live data.		
		In some cases, it may be necessary to be able to demonstrate that all information on a specific topic is available for review at any time. In this category, topics such as indexing accuracy and business continuity planning are key.		
		Ensure peripheral security issues are adequate (including buildings, temperature controls, network links, etc) and the auditable implementation of procedures by all staff are both key elements		
		The Information Security Policy Document should be approved by the organization's senior management. That approval should be documented.		
		The organization should agree and document appropriate levels of security for managing its information, in compliance with its Information Security Policy Document.		
		Information security policy document must contain at least: Scope, Statement of management objectives, policy statements, requirements for information classification categories, allocation of responsibilities, policies for dealing with breaches, policy regarding compliance with standards.		
		An agreed and approved Business Continuity plan needs		

	Procedures Manual(s)	include the topics listed below: — document capture; — document scanning; — data capture; — indexing; — authenticated output procedures; — file transmission; — information retention; — information destruction; — backup and system recovery; — system maintenance; — security and protection; — use of contracted services; — workflow; — date and time stamps; — version control; — maintenance of documentation.		
		The procedures manual must be readily accessible to appropriate users of the system.		
	Quality Control logs			
	System Description Manual (Application controls)	Details of system configurations should be documented.		
		For systems already in operation, information stored on the system prior to the achievement of compliance with the Information Management Policy Document cannot be considered as meeting its provisions unless the controls and procedures described in this Policy Document have been in place from the time of storing that information.		
	Maintenance logs			
	Contracts			
	Audit trails (Applications controls)	Records should be kept of information management system historical activities or events that may need to be reconstructed in the future, in support of stored information.		
		Audit trails should contain sufficient and necessary information to enable the demonstration of the authenticity of stored information.		
		The content of the audit trail should be agreed upon with all relevant departments within the organization.		
		The audit trail should contain data about changes to the information stored on the system.		
		In the case of audit trail data not generated automatically by the system, the procedures for generating such data should be documented in the Procedures Manual.		

		information to which it refers.		
		The audit trail should be kept at the level of security appropriate to preventing any change to any data within it.		
		Audit trail data should be stored securely in accordance with the relevant Information Security Policy.		
		Secure backup copies of the audit trail should be kept. This applies to audit trail data kept on electronic media and on paper/microfilm.		
		Audit trail information kept within the information management system should not be modifiable.		
		For least risk, audit trail data should be stored on WORM media. If a rewritable medium is used, then additional procedures need to be implemented to prevent changes being made. The use of magnetic tape will make it relatively difficult to modify data, as magnetic tape is normally a serially written medium.		
		For all system audit trail data, it should be possible to identify the process involved and the date and time of the event.		
		Where information is moved from one storage device to another, as part of a migration process, details of the move should be stored in the audit trail.		
		Information that may be stored in the audit trail typically will include:		
		— document or file identification;		
		— process date and time stamp;		
		— batch reference (for batch input);		
		— number of pages (for document scanning) or data records (data capture);		
		— quality control check approval;		
		— an identifier for each document or file that was indexed;		
		— operator or workstation identifier;		
		— final write to storage.		
		The choice of actual data to be stored in the audit trail will depend upon the application and the system.		
	Controls (Application controls)	Establish a chain of accountability and assign responsibility for activities involving management of electronic information at all levels		
	Separation of roles (Applications controls)	Ensure that the physical and managerial separations that exist around a system are mirrored by the logical access controls within it.		
	Information security management	The organization should adopt an Information Security Policy, covering all elements of the information management system. These security measures need to be aligned to any information classification categories that		

		demonstrate that all information on a specific topic is available for review at any time. In this category, topics such as indexing accuracy and business continuity planning are key		
		Ensure peripheral security issues are adequate (including buildings, temperature controls, network links, etc) and the auditable implementation of procedures by all staff are both key elements		
		The Information Security Policy Document should be approved by the organization's senior management. That approval should be documented.		
		The organization should agree and document appropriate levels of security for managing its information, in compliance with its Information Security Policy Document.		
		Information security policy document must contain at least: Scope, Statement of management objectives, policy statements, requirements for information classification categories, allocation of responsibilities, policies for dealing with breaches, policy regarding compliance with standards.		
				EDRMS
Section	**Requirement**	**Assessment details/Questions**	**Yes**	**No**
IT general controls	Information Security policy			
	Risk Assessment	The organization should undertake an information security risk analysis, and document the results obtained. A structured review of the information assets of the organization should be conducted, and risk factors assigned (based on asset value, system vulnerability and likelihood of attack). An Information Security Policy can then be produced and approved, against which security measures can be audited.		
		Risk analysis must include vulnerability based on types of media used, including live, archive, and back-ups		
		Where different types of storage media are used, their impact on the risk analysis results should be reviewed.		
		Risk review needs to be acted on to reduce risk of		

Business Continuity Planning	An agreed and approved Business Continuity plan needs to be implemented. Procedures to be used in cases of major equipment, environmental or personnel failure should be developed, tested and maintained.		
Consultations			
Compliance with procedures	Ensure that all appropriate staff have the necessary training to comply with the procedures in the procedures manual.		
	Procedures should be implemented which ensure that all staff who operate the system adhere to requirements.		
Updating and reviews	Update procedures manual with any changes. Keep all previous versions.		
	Any changes must be documented, and should include details of any change control procedures used, and procedures to ensure that the new procedures are implemented.		
	Where changes are being implemented, they should be checked to ensure that operational requirements and the requirements of the Policy Document are not compromised.		
	Superseded versions of the Procedures Manual should be kept in compliance with the Policy Document.		
	Plan, conduct and document regular reviews. An annual review should be conducted to ensure any changes to procedures or technology are reflected in the procedures manual.		
Index storage			
Index amendments			
Local area network transmission			
External transmission of files	Differences between sent and received files might be caused by errors in transmission or by deliberate alteration of one file or another. Demonstrating that a received and a sent file contain identical data is no different from demonstrating that any two copies are equivalent. The primary need is to show which file is the source, and which file is the copy; i.e. which file existed first. In some instances, this requirement can be met by comparing the times at which the two files were stored. If system time clocks are accurate (and bearing in mind differences in time zones), a received file should have been stored later than that at which the source file was transmitted. Thus, the issue becomes one of being able to demonstrate the reliability and accuracy of the timings of		

		possibility of it being suggested that the image was deliberately made illegible; this also avoids any risk of rejection of an image on the grounds that it is not a facsimile of the source document; * alternatively, a note may be stored which states that the original source document was of poor quality, and includes details of any visible information that needs to be stored; * a separate record that physical amendments or annotations were present on the original document, plus details of what the physical amendments were, may be sufficient; * where **fraud has been identified, or where litigation is envisaged or ongoing**; *** documents of high value**, such as the signed original of a large contract.		
	Information destruction	Procedures for the destruction or disposal of information at the end of the retention period should be documented. No source documents should be destroyed until the images have been successfully written to storage and appropriate backup procedures have been completed.		
	Backup and system recovery			
	System Maintenance			
	Security and protection	The audit trail should be kept at the level of security appropriate to preventing any change to any data within it.		
		Audit trail data should be stored securely in accordance with the relevant Information Security Policy.		
		Secure backup copies of the audit trail should be kept. This applies to audit trail data kept on electronic media and on paper/microfilm.		
		Audit trail information kept within the information management system should not be modifiable.		
		For least risk, audit trail data should be stored on WORM media. If a rewritable medium is used, then additional procedures need to be implemented to prevent changes being made. The use of magnetic tape will make it relatively difficult to modify data, as magnetic tape is normally a serially written medium.		
	Security procedures			
	Encryption keys and digital signatures			

	Procedures and Processes	The organization should maintain a Procedures Manual for each information management system, describing all procedures related to the operation and use of the system, including input to, operation of and output from the system.		
		Procedures Manual. The Procedures Manual should include the topics listed below: — document capture; — document scanning; — data capture; — indexing; — authenticated output procedures; — file transmission; — information retention; — information destruction; — backup and system recovery; — system maintenance; — security and protection; — use of contracted services; — workflow; — date and time stamps; — version control; — maintenance of documentation.		
		The procedures manual must be readily accessible to appropriate users of the system.		
	Maintenance of documentation			
	Storage media and sub-system considerations	Image files stored on magnetic disk and other random access rewritable media may, in principle, be modified. With such media, the risk of modification is less to do with the medium itself than with the controls that are implemented by the storage sub-system and by the access software. The ability to alter files requires read-write access, and well-designed systems have controls to prevent unauthorized read-write access. Users with read-only access are unable to modify the files. This alone is unsatisfactory unless the system also maintains a secure record of all read-write accesses. In a system where there are very frequent file modifications, there may be a substantial overhead to record these modifications, but if a record is not kept, it might prove impossible to detect any unauthorized alterations by a skilled hacker or by anyone with the appropriate access privilege.		
	Access levels (Application controls)	Only staff with the relevant access rights should be permitted to enter or amend stored information.		
	Digital and electronic signatures including biometric			

	Audit trail information (Application controls)	For all system audit trail data, it should be possible to identify the process involved and the date and time of the event.		
	Stored information			
	Change control			
	Digital signatures (Application controls)	Digital signatures, keys and algorithms should be stored securely, and access to them should be allowed only to authorized personnel.		
	Destruction of information			
			0	0
				EDRMS
Section	**Requirement**	**Assessment details**	**Yes**	**No**
Application Controls	Document image capture			
	Document scanning procedures			
	Data Capture			
	Indexing			
	Authenticated Output procedures	Such procedures may, for example, require the use of standard system features for copying, and written confirmation by an authorized person that the copying process has been conducted correctly. The procedures may specify how authenticated copies are subsequently to be handled. The procedures may refer to audit trail data as a confirmation of the processes that occurred during copying.		
		Where a physical document is produced as part of the output, the procedures should include the use of an authorized signature or other procedure to authenticate this copy document.		
	Preparation of paper documents (IT general controls)			
	Document batching (IT general controls)			
	Photocopying (IT general controls)			
	Scanning processes (IT general controls)			
	Quality control (IT general controls)			
	Evaluating Image Quality			
	Checking Scanner performance			
	Rescanning			

	New data			
	Migration			
	Indexing			
	Manual Indexing			
	Automatic Indexing			
	Index Accuracy			
	File transmission			
	Intra-system data file transfer			
	Scanning systems			
	Workflow			
	System Description Manual	Details of system configurations should be documented.		
		For systems already in operation, information stored on the system prior to the achievement of compliance with the Information Management Policy Document cannot be considered as meeting its provisions unless the controls and procedures described in this Policy Document have been in place from the time of storing that information.		
	System Integrity checks	To protect stored information from malicious software, appropriate protection software should be installed and kept up to date		
	Image Processing	Where it is important that there should be no loss of information in the scanned image, other than that due to the scanning resolution, there should be no image processing subsequent to the initial creation of the image file.		
	Compression techniques			
	Migration	There should be provision for migrating electronic files, including metadata, index data and audit trails, to new technology without loss of integrity, and with sufficient migration process documentation to allow the integrity of the stored information to be established at any time in the future.		
	Information deletion and/or expungement	Where deletion and/or expungement is implemented, appropriate authorization should be obtained prior to the action being implemented.		
	Audit trail data	Records should be kept of information management system historical activities or events that may need to be reconstructed in the future, in support of stored		

	Creation	In the case of audit trail data not generated automatically by the system, the procedures for generating such data should be documented in the Procedures Manual.		
	Date and time	Each audit trail data record should have an associated date and time, which relates to the date and time of the event being stored.		
	System			
	Migration and conversion	Where information is moved from one storage device to another, as part of a migration process, details of the move should be stored in the audit trail.		
	Information Capture	Information that may be stored in the audit trail typically will include:		
		— document or file identification;		
		— process date and time stamp;		
		— batch reference (for batch input);		
		— number of pages (for document scanning) or data records (data capture);		
		— quality control check approval;		
		— an identifier for each document or file that was indexed;		
		— operator or workstation identifier;		
		— final write to storage.		
		The choice of actual data to be stored in the audit trail will depend upon the application and the system.		
	File Information			
	Scanned Document Information (IT general controls)			
	Batch information			
	Indexing			
	Workflow			
			0	**0**
				EDRMS
Section	**Requirement**	**Assessment details**	**Yes**	**No**
Substantive test on the record	I. Using the National Archives and Records Service metadata requirements to consider the risks if you cannot show:	Can or will you be able to prove the information is authentic?		
	* Who created it			

	* A user accesses part of the record without realising there is more relevant information	When you access a record, can or will you be able to access all relevant parts of it?		
	* Decisions are made based on incomplete information when additional information is available.			
	IV. The National Archives and Records Service metadata requirements require the following metadata elements: particular identity, context, relationships, date information, version control, access control, disposal control, record type, presentation and medium, location information, system information, vital record information and audit information			
		Is the template used dated?		
		When acting is there a scanned letter confiirming that?		
		Is there consistency when completing information?		
		Is there a control regarding signatures?		
		Is there a process regulating externally generated records?		
			0	**0**

Assessed by:	
Assessment recommendations:	
Reviewed by:	
Date of next review:	