Ingesting digital archives into long-term storage system through free open-source software in South Africa

Mahlatse Moses Shekgola
Department of Information Science, University of South Africa – Muckleneuk Campus, Pretoria, South Africa, and
Mpho Ngoepe
Department of Information Science, University of South Africa College of Human Sciences, Pretoria, South Africa

Abstract

Purpose – In South Africa, public institutions face challenges in transitioning their digital records to trusted digital repositories due to a deficiency in skills, infrastructure and systems. Free and open-source software (FOSS) presents a viable solution for facilitating the transfer of digital archives for permanent preservation. Despite the existence of FOSS policy in South Africa, the public sector has yet to fully use it to engage in the development and implementation of products for records management and archive preservation using open-source software. This study aims to explore the ingestion of digital archives into an approved long-term storage system through FOSS in South Africa with the view of developing a framework.

Design/methodology/approach – The study adopted a qualitative research approach to collect data through interviews with purposively selected participants (records managers, archivists and IT officials) from national government departments that have implemented records management systems for digital curation of archives, as well as the National Archives and Records Services of South Africa (NARSSA), which regulates archives and records management, and the State Information Technology Agency, which regulates information technology in government.

Findings – The findings of the study suggest that the systematic transfer of digital materials from public entities to NARSSA, as required by statute, has not taken place.

Research limitations/implications – The study specifically targeted national government departments that have implemented digital archives and records management systems. Consequently, perspectives from departments that have not implemented these solutions were excluded.

Originality/value – A framework is proposed for the transfer of digital archives, using interoperable FOSS, from government agencies responsible for records management to NARSSA for archival preservation. This framework, it is hoped, will facilitate infrastructure and skills development in the management of records and preservation of archives through open platforms.

Keywords Digital repository, FOSS, Proprietary software, Security, Interoperability, Digital records

Paper type Research paper

Introduction and background to the study

The persistent lack of infrastructure for preserving digital archives by NARSSA has left public entities that have adopted electronic records management systems in a quandary, unsure of how to handle records of enduring value that should be transferred to archival repositories. As Katuu (2012) points out, valuable records are prone to damage, loss and degradation over time due to insufficient capacity, security measures, skills and technology, among other factors, for their preservation. In a country with a free and open-source software (FOSS) policy, public entities should seise the opportunity to develop their own infrastructure, which would also foster local skills. As a result, FOSS can provide both creating agencies and archival institutions with the necessary technology and infrastructure for transferring digital records of lasting value to archival custody in accordance with legal requirements. Notably, FOSS technology and infrastructure may prove indispensable for NARSSA, which grapples with reliable tools for the transfer and preservation of digital archives (Ngoepe, 2017). NARSSA's records system caters to two types of records, as outlined by Ngoepe (2017): those slated for destruction after a specified period, typically within 20 years, and those with enduring value necessitating permanent preservation in archival repositories after two decades. This mandate, as Ngoepe and Kenosi (2022) assert, aligns with Jenkinson's primary and secondary roles of archivists regarding records. In the primary role, records are managed within creating agencies, while in the secondary role, those with

The current issue and full text archive of this journal is available on Emerald Insight at: **https://www.emerald.com/insight/2514-9326.htm**

Collection and Curation
44/1 (2025) 25–33
Emerald Publishing Limited [ISSN 2514-9326]
[DOI 10.1108/CC-02-2024-0003]

Received 13 February 2024
Revised 23 April 2024
Accepted 23 April 2024

enduring value are transferred to archival repositories. Digital records of enduring value also require transfer to archival repositories, a practice not yet established in South Africa due to the lack of infrastructure, despite the passage of a FOSS policy by the cabinet in 2003. As FOSS continues to evolve rapidly within the information and communications technology (ICT) industry (Drake, 2017), this study posits that the software can contribute to IT skill development, cost-effectiveness, security and compatibility, among other benefits, for South Africa.

This study intends to explore the ingestion of digital records into archival custody through free open-source software in South Africa, with a focus on the national government departments and NARSSA. The study argues that digital records of enduring value created and managed by national government departments warrant a systematic transfer to an archival institution for permanent preservation when their administrative purposes are no longer needed.

Problem statement

Public entities in South Africa lack adequate and reliable facilities that offer systematic transfer of digital materials from creating agencies for permanent preservation to archive repositories. This tends to lead to the disappearance and loss of valuable records in the hands of creating agencies due to their lack of necessary skills, security and technology relating to long-term preservation (Shibambu and Ngoepe, 2020). Even the creating agencies that have employed the usage of cloud storage as a temporary measure for their digital materials are struggling and facing issues relating to limited storage capacity on their local servers. Moreover, the security of valuable records is in danger emanating from cybercriminals, authorised and unauthorised users who may deliberately temper with the records in unsecured systems (Ngwenya and Ngoepe, 2022). This is a result of the perception that many government departments still use outdated software and hardware to run their records management systems.

FOSS implementation may offer swift transfers of records from creating agencies to archival institutions. FOSS solutions and systems often adhere to open standards and can integrate seamlessly with other tools and systems commonly used in digital curation, promoting data exchange and collaboration (Gupta and Surbhi, 2018). This offers the interoperability of various software. Interoperability may facilitate the easy transfer or migration of digital records from FOSS to proprietary systems and vice versa (Rezaei *et al.*, 2014). In this case, FOSS implementation for digital curation of archives in national government departments may ensure compliance with relevant laws and regulations related to universally accepted principles. These standards may therefore enable the swift transfer of records from one national government department to another (Rezaei *et al.*, 2014). Most importantly, the ingestion of digital records required by standards and principles may play a significant role in the transfer of digital archives from the national government department to the NARSSA for permanent preservation. FOSS can ensure that records management systems share and transfer digital records from one point to another (Svärd, 2013). This is important in the distribution of digital records with enduring value for permanent preservation, especially from the creating agency (McKemmish, 2017). As supported by the records lifecycle model, the inactive stage of records may call for records to be transferred to an archival repository for permanent preservation (Lin, 2015).

Purpose and research objective

The purpose of the study is to explore the ingestion of digital records into long-term storage systems through free open-source software in South Africa. The specific objectives are as follows:

- determine implemented software for digital records and archives management in South Africa;
- assess the security measures required for long-term storage of digital archives in South Africa; and
- propose a framework for FOSS implementation towards the ingestion of digital records in archival custody.

Literature review

The literature review of this study is based on themes from the objectives of the study.

Software implemented for long-term storage of digital archives

As alluded to by the record's lifecycle model, the software implemented for digital records plays a significant role throughout their lifespan. This software, whether proprietary or open-source, should be able to cater to the creation, distribution, use, maintenance, disposal and long-term preservation of archives (Lin, 2015). Most importantly, as alluded to by the records lifecycle model, the implemented software should be able to facilitate the transfer of records to various organisations and back, as well as to the archival repository when the need arises. As such, the implemented software in digital records should be regarded as the key technological aspects that drive the existence of records and their records management systems.

The proliferation of technology has brought about a paradigm shift in the sphere of record management and preservation. This is bound to force organisations in the modern era to create, receive, maintain, use, dispose of and preserve records in the form of digital records (Digital Preservation Coalition, 2022). Such includes records that are digitised from paper format as well as born digital. Born digital are records that have been natively created in a digital format by means of computers. They are created using office applications such as word-processed documents, spreadsheets and multimedia presentations. Other digital records include images and videos, social media, websites and email. These records need to be managed and preserved in systems that will ensure continued access, retrieval and use. For instance, records emanating from emails require management and preservation. Email records are the result of automating correspondence. According to the Digital Preservation Coalition (2022), email offers singular insight into and evidence of a person's self-expression, as well as records of collaboration, networks and transactions.

However, looking at the impact of FOSS on the African continent, Katuu (2012) as well as Ngoepe (2015) have noted with concern that, although there seems to be interest, particularly in the sphere of digital records management and preservation, many countries are still hanging on to the proprietary software. Katuu (2012) alludes to the fact that this may be caused by the fact that, since the initial phase of management and preservation of digital records, proprietary software has been deemed the preferred choice. Such FOSS solutions include AtoM, Alfresco, Archivematica, Epadd, Greenstone and DSpace, to name just a few. On the other hand, Ngoepe (2015) points out that proprietary software, comprising Hummingbird and Livelink, amongst others, still reigns supreme in most governmental bodies in South Africa. This continues to occur despite drafted policies that are adopted with the aim of replacing the use of proprietary software with or by implementing FOSS solutions (Ngoepe, 2015).

However, as supported by Akintomide (2016), various archival institutions around the world are reaping the benefits of implementing open-source software solutions, particularly in their bid to address issues related to the ingestion of digital records into archival custody. As such, these governments migrated to open-source software products that provide them with the option of a detailed review of the source code to fix problems themselves without waiting for the vendor. On the other hand, some countries moved to FOSS due to benefits that include lower software costs, escaping vendor lock-in, transparency of data and record longevity, skills development, scaling and consolidation potential, support, security and quality software (Bwalya *et al.*, 2019).

Security measures for long-term storage of digital archives

Robust security to ensure integrity and swift transfer of records from creating agencies to archival institutions can never be overemphasised. The security of digital archives is essential in ensuring that such material remains accessible, usable, transferable and can be used over long periods of time (Ngwenya and Ngoepe, 2022). The records lifecycle model emphasises that the main reason for the curation of archives, particularly when it comes to digital records, is to safeguard continuous access to these records whenever a need arises (Lin, 2015). However, ensuring security for large and ever-expanding collections of digital materials has proven to be a mammoth task for archival institutions around the world (Corrado and Moulaison, 2014). Digital records are fragile materials that must be handled in a manner that ensures they are secure.

Unfortunately, in various public institutions, such as archival repositories and governmental bodies, vast amounts of digital records are stored in an unstable digital environment (Ngoepe, 2017). In some instances, ARM systems are left to be attacked by security threads due to a lack of implementable, robust security features. Unprotected or vulnerable ARM systems tend to allow malicious people to access digital as well as place classified and confidential records at risk of being tampered with (Ngwenya and Ngoepe, 2022). This is because many government institutions around the world tend to implement very little security on their systems and thus become exposed to and are targeted by cybercriminals owing to resource deficiency such as insufficient budgets (McHugh, 2021). As such, these sophisticated criminals continue to exploit vulnerable records management systems that contain valuable digital records for their own benefits.

FOSS can provide more secure, dependable and less costly technology when it comes to security. According to Karume and Mbugua (2012), this is because FOSS products provide users with the option of a detailed review of the source code, giving users the ability to fix problems themselves without having to wait for the vendor. On the other hand, proprietary products that are often rented tend to be packed with security vulnerabilities (Buffett, 2014). Hence, according to Techopedia (2012), Linux (a FOSS operating system) is perceived to be the leading technology because it is seen as more dependable and safer than Microsoft Windows (a proprietary operating system). Therefore, the attainment of the Linux operating system (for example) makes the concept of FOSS attractive to various organisations that deal with information and communication technology activities.

Security to ensure systematic and seamless transfer of digital records, particularly in digital systems, ensures that records are kept in their original format as created or received and securely against possible alteration. The record lifecycle models point out that the access, use and reuse of digital records heavily depend on the safety of the digital systems in which they are stored (Lin, 2015). In this way, the safety of systems enables the continual utilisation, access and distribution of digital records, which are the fundamental requirements of the records lifecycle model. This thus calls for the implementation of robust actions and techniques to mitigate possible threads that may hamper the transfer of digital records (Ngwenya and Ngoepe, 2022).

Reliability of digital records is concerned with establishing the dependability of a record as a statement of fact by examining the completeness of the record's form and the amount of control exercised in the process of its creation (Cheng *et al.*, 2019). A record is deemed reliable when it can be treated as a fact, that is, as the entity of which it is evidence. The authenticity and reliability of digital records in a records management system convey the trustworthiness of records. This means that digital records kept in the system contain accurate statements of facts and a genuine manifestation of those facts. As asserted by Ngwenya and Ngoepe (2022), some security measures that should be guarded against include the following: file format and technology obsolescence, human errors by both authorised and unauthorised staff and cybersecurity. The security concerns are discussed below:

File format and technology obsolescence

File format and technology obsolescence are leading security concerns in the digital curation of archives due to the fact that the technology in which these records are created, used, shared and subsequently preserved constantly changes with technology. This factor thus makes it imperative for organisations to keep up with the ever-changing technology pertaining to systems, software and hardware that are used for the management of records (Wanyonyi *et al.*, 2017). Old machines as well as storage media may be superseded by new technology and devices. In most cases, technology obsolescence in digital record-keeping systems may result in records being no longer accessible, particularly if they were not copied to new

devices (Cheng *et al.*, 2019). Technology obsolescence may also occur on hardware as well as software. When hardware becomes obsolete, equipment usually wears out, cables and other components may go missing and the machine may also fail to turn on and off (Cheng *et al.*, 2019). On the other hand, the software may fail to open the system to files. The same problem may occur in the case of file format obsolescence. File format obsolescence occurs when the software for reading the file format is no longer available. Files can become corrupted in the event of hardware or software failure.

Therefore, to secure and preserve the longevity of digital records, organisations may deploy strategies such as migration or emulation to ensure that they can still be used in future technologies and devices (McHugh, 2021). OpenDocument Format (ODF), a FOSS file format, stems from the open XML-based OpenOffice.org specification and was also approved by ISO as a standard in 2006 (Gupta and Surbhi, 2018). In terms of guaranteed long-term availability, international standards bodies have rendered ODF the safest file format (Gupta and Surbhi, 2018). Moreover, FOSS involves representatives from different constituencies to be involved in creating the standard, helping to ensure that it balances the needs of a wide variety of users and that it is not obligated to any commercial interest.

Human error, authorised and unauthorised staff

Digital archives are prone to human error through the accidental or deliberate tempering of important records by both unauthorised and authorised individuals. Staff with legitimate access rights commit fraud and sabotage IT infrastructure, making it difficult to achieve security (Cheng *et al.*, 2019). In most cases, it is difficult to track down the culprit. Security around authorised and unauthorised staff is therefore very important in digital records management and in repositories to guard against malicious damage, loss, forgery and theft and to ensure that records are kept according to depositor and user's needs (Wanyonyi *et al.*, 2017). Records can be protected by having security measures in place to secure them against unauthorised access.

As with physical records, human error is a threat to the security of digital record systems. To curb this problem, it is important that people with suitable security clearance be allowed to access and use digital record systems. Time-out periods should be implemented on the system just in case a user forgets to logout of the system after use (Wanyonyi *et al.*, 2017). Furthermore, the system should allow only authorised people to key in the correct password to access records. The use of passwords to access digital records may ensure that records are not exposed to unauthorised people. Since digital records are sensitive and fragile to security, it is also important that organisations continuously conduct risk assessment, storage media and disaster preparedness as fundamental ways of addressing security issues.

Cybersecurity

The biggest security thread in digital records management and preservation systems emanates from the ever-increasing breaches by cybercriminals. Cybersecurity is concerned with the application of technologies, processes and controls to protect systems, networks, programmes, devices and data from cyberattacks (McHugh, 2021). The goal is to reduce the risk of cyberattacks and exploitation of systems by cybercriminals. The breaching of digital record systems tends to expose records, including confidential records such as health and financial records (Cheng *et al.*, 2019). Implementing the proper security measures to make sure that valuable records are not vulnerable to a breach and tempering by cybercriminals should be one of the top priorities of any organisation. Apart from cybercriminals, systems may be exposed to cyberthreats such as malware, including trojans, worms and viruses; crypto-jacking, which installs illicit cryptocurrency mining software; form-jacking, which inserts malicious code into systems; and backdoors, which allow remote access (Cheng *et al.*, 2019).

Therefore, it is important that digital record-keeping systems are constantly updated, upgraded and installed with the latest security features to enable the detection and prevention of unauthorised activities in the network and systems to keep the information intact (McHugh, 2021). Access and security issues must be given proper attention because unprotected digital record systems can be hacked by cybercriminals (Ngwenya and Ngoepe, 2022). This can be achieved by implementing minimum authentication controls, such as user accounts used to log into the records-keeping systems and ensuring that only appropriate users are permitted access. Wanyonyi *et al.* (2017) point out that databases containing personal, financial and medical records that are useful to both individuals and organisations should also be safeguarded. This is important to curb accidental or intentional violations of the right to privacy.

Methodology

This qualitative study triangulated interviews with document analyses to explore the ingestion of digital records into archival custody through free open-source software in South Africa. Interview data were collected from records managers and chief information officers from purposively selected public entities that have implemented electronic content management, as well as archivists and IT officials from the NARSSA and State Information Technology Agency (SITA), responsible for archival system implementation. The NARSSA and SITA were contacted to provide the names of national government departments that have implemented systems for digital records management and preservation in South Africa. These two organisations usually work hand in hand with governmental bodies that manage digital records in South Africa. Directors and, in some instances, chief directors of each department were contacted to acquire permission to conduct the study in the institution. The key measure based on which the population of this study was selected was that they worked relatively close to digital records management and preservation in their respective organisations. For instance, archivists and records managers are tasked with performing a strategic and executive role on records, including digital records, as part of their key duties. At times, they are accountable for the digital curation of archives. As such, the decision to choose archivists and records managers in this study was because they were able to share their knowledge and expertise on the software implemented for the digital curation of archives and, ultimately, the preservation of such records. As reflected in Table 1, semi-structured interviews were conducted with 13 participants, including records managers, archivists and

Table 1 Implemented software in digital curation of archives

Participants	Software currently implemented	Type of software	Functional use of the solution
ARMP-1 and ICTP-1	Alfresco	Open source	Records management
RMP-2 and ICTP-2	AToM	Open source	Archival solution
RMP-3 and ICTP-3	FileDirector and SmartGov	Proprietary	Records management
RMP-4 and ICTP-4	SmartGov	Proprietary	Records management
ARMP-5 and ICTP-5	Alfresco	Open source	Records management
ARMP-6 and ICTP-6	Archivematica	Open source	Archival solution
ARMP-7	Documentum	Proprietary	Records management

Source: Authors' own work

IT specialists. Data were analysed and presented thematically with the use of word clouds, figures, tables and *verbatim* quotations, as in line with the objectives of the study.

Findings and discussion of data

The findings and discussion of data are presented through figures, tables, word clouds and *verbatim* quotes. This section is presented according to themes emanating from the research objectives.

Solutions implemented for long term storage of digital archives

The objective of this study was to examine the software currently implemented by national government departments and NARSSA for the digital curation of public archives. This focus arises from the prevailing literature highlighting the benefits experienced by numerous governments worldwide upon adopting and implementing FOSS solutions for digital archive curation. However, it appears that countries like South Africa have not fully capitalised on FOSS technology, particularly in the context of digital archive curation. This observation aligns with the findings of Ngoepe's (2015) study, which revealed that only two national governments in South Africa had implemented FOSS solutions. Participants in Ngoepe's study expressed the need for legislation promoting FOSS implementation, seen as a potential catalyst for its adoption and use within governmental bodies.

While this is still the case, Table 1 shows that the organisations that were part of the study have been consistently adopting FOSS-based solutions, especially for digital archive curation in South Africa. This is different from the report by Ngoepe (2015). Notably, NARSSA sets a positive example by embracing open-source preservation and access solutions, such as Archivematica and AToM. However, it is important to highlight that NARSSA has yet to test these solutions for ingesting digital records into archival custody by creating agencies. Thus far, the focus has been on digitising analogue records and making them accessible through AToM.

Security measures for long-term storage of digital archives

Robust security measures play a crucial role in ensuring the accessibility, usability and reusability of digital records in systems. Digital records are normally stored in electronic records management systems, which are liable to security threats emanating from various internal and external factors. The security of records managed in such systems, especially by government institutions, is increasingly faced with possible breaches and attacks from cybercriminals. As revealed by Corrado and Moulaison (2014), the deployment of key mitigation approaches is necessary to ensure that the information contained in records management systems remains accessible, retrievable and, most importantly, secured from possible intruders.

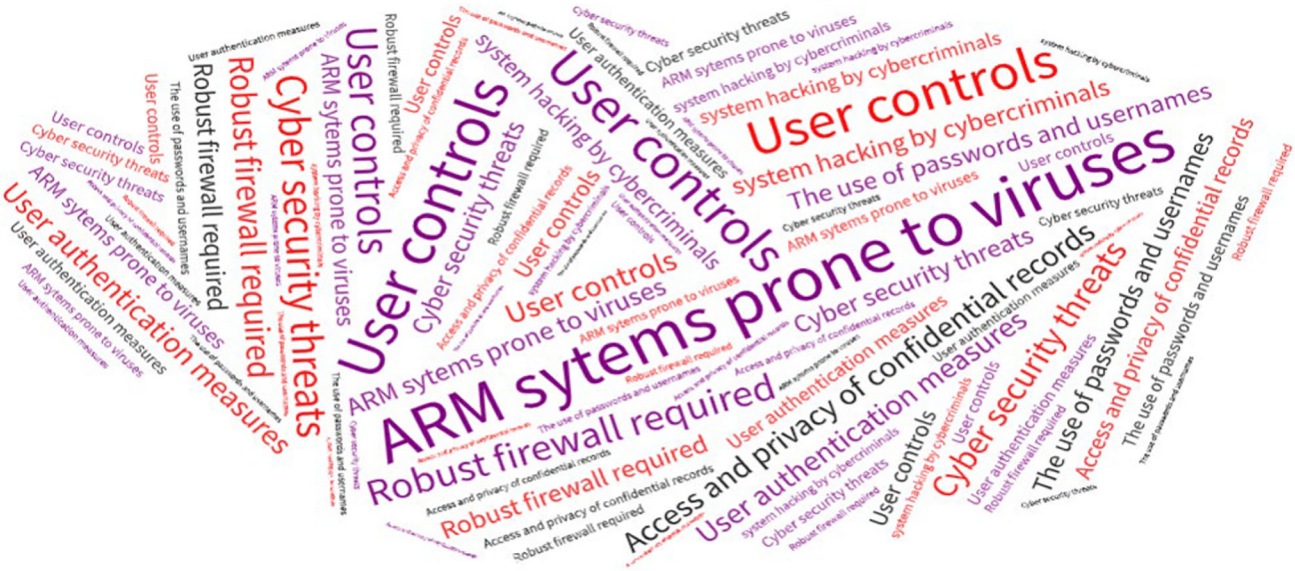
As illustrated in Figure 1, a cloud of security concerns experienced by participants in the digital curation of archives throughout their respective organisations are highlighted. The prominent words include user control, viruses, confidential records, cyber security threats, firewalls and password control. Participants point out that they sometimes feel uncertain about the levels of security in the records management system, owing to the stated issues.

Likewise, participants have indicated that they have used mitigating tactics to curb security threats that may emanate from cybercriminals in the form of hacking digital systems as well as bridging the firewalls of such storage facilities. It emerged in the current study that most national government departments are struggling to safeguard their systems with sophisticated protective measures due to a lack of sufficient budget.

Even with the limitation of budget towards implementing vigorous preventative approaches to records management, participants have indicated that they are doing fairly well to mitigate threats. It was also revealed by the participants of the study that various user controls for unauthorised access and retrieval of digital curations of archives are usually put in place. Some of the user controls mentioned included the use of usernames and passwords to log into systems to verify authentication for users of the digital curation of archives. This tactic is commonly used in national government departments to ensure that access to the system is granted to the right user.

Participants indicated that they had never experienced any harm caused by cybercriminals. Similarly, participants who implemented FOSS provided that they deemed their records management safe and secure. These participants mentioned that their records management systems were never bypassed by intruders due to their stability. Literature also showed that FOSS systems tend to be superior in terms of security as opposed to proprietary software. This is mainly due to constant improvements made by the FOSS community and software developers, who can view, alter and improve various versions

Figure 1 Security concerns for long-term storage of digital records



Source: Shekgola and Ngoepe 2024

that are released. In this way, it becomes easier to detect issues beforehand, so that the final product may be safe for all users.

However, participants in the study have concerns about the lack of interoperability of systems. The interoperability of solutions is about bringing together various applications and ensuring that they can function in sync, allowing easy collaboration and information sharing. Participants alluded to experiencing issues relating to the interoperability of solutions and records management systems, especially in the software currently implemented by both national government departments and NARSSA to facilitate the swift transfer of digital curation of archives to one another. Participants from the NARSSA and SITA indicated that the systems have never been tested for interoperability and the transfer of digital records.

Participants have indicated that it is worrisome that most organisations seem to have implemented different types of solutions for the digital curation of archives. Participants seem to concur that regulating agencies such as SITA and NARSSA have a role to play in ensuring that at least all government departments implement and use one solution for records management. Moreover, the study discovered that most ICT personnel interviewed were part of the Government Information Technology Officers Council (GITOC), which is a council responsible for the management and utilisation of information and IT resources across the government of South Africa. These participants agree that the implementation of a uniform solution for governmental use may be beneficial in various ways. Participant ICTP-4 opined that:

> SITA together with GITOC and NARS need to sit down identify one best solution for use by all national government departments. Once that is done, the two will have to layout implementation plan across all government department. And if the identified solution is open-source software, they need to make sure that issues such as support, and skills are addressed and ensured to each department.

ICTP-5 also agrees that GITOC and SITA have a role to play, more so if national government departments are to realise the use and implementation of a singular solution in the digital curation of archives. The participant laments the variety of databases caused by various solutions implemented by the national government. The participant rates retail stores as way better organised than most government systems. The participants point out that:

> Database implemented by retail stores are much integrated, and consumers are spoilt for choice because the systems are integrated than in government. You are likely to buy a bus ticket from retail store X, Y or Z, since its one system. In government, it is not that organised.

When asked what the solution could be, ICTP-5 said:

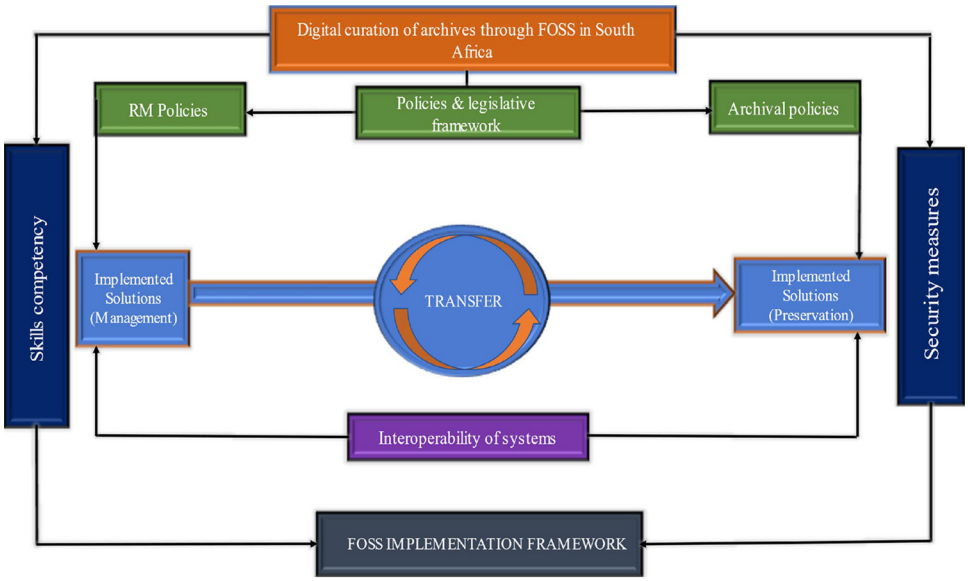
> SITA and GITOC need to find a consolidated effort in terms of what is it that we need to do as government departments. We need to find a way to come together and stop working in silos even though we meet, and we discuss challenges. At the moment there's a gap in terms of consolidated effort. So, I think that's what we need to work on.

Proposed framework for FOSS implementation for ingestion of digital records

This section introduces the proposed framework for the ingestion of digital archives into a long-term storage system through FOSS implementation. The study reveals that national government departments in South Africa have yet to systematically initiate the transfer of their digital archives for permanent preservation due to lack of infrastructure. Consequently, valuable digital records that may merit preservation in the national archives remain within their respective departments. Several factors, including the absence of FOSS legislation, inadequate infrastructure for preserving digital materials and a lack of system interoperability and mechanisms to facilitate swift transfer to and from creating agencies, have hindered the ingestion of digital materials into archival custody.

The proposed framework, depicted in Figure 2, encompasses the following key components: archival policy and legislative framework; and interoperability of records management solutions

Figure 2 Digital curation of archives through FOSS



Source: Shekgola and Ngoepe 2024

for transferring digital records into archival custody. Achieving this requires essential archivist skills and ensuring system security.

The proposed framework for the long-term storage of digital archives through FOSS relies heavily on the presence of a FOSS policy and supportive legislation, facilitating its adoption within creating agencies and archival institutions. As such, key role players such as NARSSA and SITA, should be engaged first. This is to ensure that the software implemented and used for ingestion of records are based and governed by legislative framework, policy and standards as prescribed the two bodies. This further entails using software that adheres to legal frameworks, policies and standards for record transfer, which are crucial elements of any records management division or section. Such legal frameworks provide structured approaches to ensure compliance and guide actions. Legislation supporting FOSS for the transfer of digital curation of archives establishes rights, responsibilities and penalties for non-compliance, thereby playing a vital role in governance.

Within the suggested framework, it is imperative to implement FOSS when creating agencies for electronic records management, marking the beginning of the records' lifecycle. These systems should be compatible with NARSSA's preservation solution for seamless transfer to archival custody once the records mature as per archival legislation. Interoperability of implemented software and digital curation of archives systems is crucial for efficient record transfer. Interoperability ensures swift exchange of records between creating agencies and archival institutions, ensuring accessibility and sustainability over time. This involves different systems and software working together seamlessly to exchange information effectively.

In addition, the transfer of archives through FOSS may necessitate practitioners possessing a certain level of skills and knowledge to ensure record security. Competent archivists and records managers can ensure robust security measures are in place to maintain the original format and trustworthiness of records during transfer. Given the susceptibility of digital curation to security threats, it's vital to implement preventative measures to mitigate potential breaches. Competent staff can adapt and use FOSS according to the requirements of the Free Software Foundation, ensuring adherence to standards and protocols.

Conclusion

The central thesis of this study asserts that FOSS implementation holds the potential to facilitate the ingestion of digital records into archival custody. Indeed, the adoption of FOSS for digital curation of archives can yield substantial benefits for both national government departments and NARSSA. The study delineates various FOSS solutions in the realm of archives and records management, such as DSpace, Alfresco, Archivematica and AtoM. Consequently, selecting the appropriate solution for digital archive curation should align with the core objectives of each national government department.

Furthermore, given the susceptibility of digital archive curation to various security threats, it is imperative to adequately plan for potential theft and threats that may jeopardise digital records. Beyond ensuring the swift transfer of records from national government departments to NARSSA, the interoperability of systems can ensure the accessibility and sustainability of digital archives over time.

As emphasised in this study, FOSS holds the potential to provide both creating agencies and archival institutions with the requisite technology and infrastructure for digital archive curation. This could be particularly crucial for NARSSA, given its challenges with infrastructure for digital archive preservation. Given the current economic circumstances in South Africa, this study further advocates for the implementation of FOSS for digital archive curation as a pragmatic approach to reducing costs associated with procuring proprietary software. By doing so, these entities could lessen their reliance on international corporations and potentially foster the development of indigenous ARM solutions, thereby playing a significant role in the realm of software development.

The study suggests a framework for the transfer of digital archives through interoperable FOSS from government agencies (records management) to NARSSA (archives). It is anticipated that such a framework will contribute to infrastructure and skills development in the management of records and the preservation of archives using open platforms. Consequently, the utilisation of FOSS in this context may offer national government departments as well as NARSSA a dependable technology to ensure the swift transfer of records between both ends when the need arises.

References

Akintomide, O.A. (2016), "A study of Nigerian librarians' attitude to open-source software", available at: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3709&context=libphilprac (accessed 12 October 2023).

Buffett, B. (2014), "How IT can contribute to changing organizational culture: factors influencing open-source software adoption in public sector national and international statistical organizations", Meeting on the Management of Statistical Information Systems (MSIS 2014): (Dublin, Ireland and Manila, Philippines 14-16 April 2014).

Bwalya, T., Akakandelwa, A. and Dobreva-McPherson, M. (2019), "Adoption and use of free and open-source software (FOSS) globally: an overview and analysis of selected countries", available at www.researchgate.net/publication/337318071Adoption_and_Use_of_Free_and_Open_Source_Countries (accessed 16 January 2023).

Cheng, X., Fu, S., Sun, J., Bilgihan, A. and Okumus, F. (2019), "An investigation on online reviews in sharing economy driven hospitality platforms: a viewpoint of trust", *Tourism Management*, Vol. 71, pp. 366-377, doi: 10.1016/j.tourman.2018.10.020.

Corrado, E.M. and Moulaison, H.L. (2014), *Digital Preservation for Libraries, Archives, and Museums*, Rowman & Littlefield Publishers, Lanham, MD.

Digital Preservation Coalition (2022), "Digital preservation handbook", available at: www.dpconline.org/handbook (accessed 3 July 2023).

Gupta, D. and Surbhi, G. (2018), "Adopting free and open-source software (FOSS) in education: I-manager's journal of educational technology", available at: https://eric.ed.gov/?id=EJ1179515 (accessed 15 January 2023).

Karume, S. and Mbugua, S. (2012), "Trends in adoption of open-source software in Africa", *Journal of Emerging Trends in Computing and Information Sciences*, available at: www.cisjournal.org/journalofcomputing/archive/vol3no11/vol3no11_10.pdf (accessed 24 January 2023).

Katuu, S. (2012), "Enterprise content management (ECM) implementation in South Africa", *Records Management Journal*, Vol. 22 No. 1, pp. 37-56.

Lin, C.Y. (2015), "Toward a holistic model for the management of documents, records, and archives", *Archival Issues*, Vol. 37 No. 1, pp. 21-47.

McHugh, R. (2021), "Different types of security in records management", available at: www.recordnations.com/2019/01/different-types-security-in-records-management/ (accessed 12 August 2022).

McKemmish, S. (2017), "Recordkeeping in the continuum: an Australian tradition", In Gilliland, A.J., McKemmish, S. and Lau, A.J. (Eds), *Research in the Archival Multiverse*, Monash University Publishing, Clayton, pp. 122-160.

Ngoepe, M. (2015), "Deployment of open-source electronic content management software in national government departments in South Africa", *Journal of Science & Technology Policy Management*, Vol. 6 No. 3, pp. 190-205, doi: 10.1108/JSTPM-05-2014-0021.

Ngoepe, M. (2017), "Archival orthodoxy of post-custodial realities of digital records in South Africa", *Archives and Manuscripts*, Vol. 45 No. 1, pp. 31-44, doi: 10.1080/01576895.2016.1277361.

Ngoepe, M. and Kenosi, L. (2022), "Confronting Jenkinson's canon: reimagining the 'destruction and selection of modern archives' through the Auditor-General of South Africa's financial audit trail", *Archives and Records*, Vol. 43 No. 2, pp. 166-176, doi: 10.1080/23257962.2022.2048639.

Ngwenya, M. and Ngoepe, M. (2022), "Data trust in consumer internet of things assemblages in the mobile and fixed telecommunication operators in South Africa", *South African Journal of Information Management [Online]*, Vol. 24 No. 1, pp. 1-9, doi: 10.4102/sajim.v24i1.1426.

Shibambu, A. and Ngoepe, M. (2020), "When rain clouds gather: digital curation of South African public records in the cloud", *South African Journal of Information Management*, Vol. 22 No. 1, pp. 1-9, doi: 10.4102/sajim.v22i1.1205.

Rezaei, R., Chiew, T.K., Lee, S.P. and Aliee, Z.S. (2014), "A semantic interoperability framework for software as a service system in cloud computing environments", *Expert Systems with Applications*, Vol. 41 No. 13, pp. 5751-5770, doi: 10.1016/j.eswa.2014.03.020 (accessed 28 August 2021).

Svärd, P. (2013), "Enterprise content management and the records continuum model as strategies for long-term preservation of digital information", *Records Management Journal*, Vol. 23 No. 3, pp. 159-176.

Techopedia (2012), "Open source: too good to be true?", available at: www.techopedia.com/2/28968/software/open-source-is-it-too-good-to-be-true (accessed 25 May 2023).

Wanyonyi, E., Rodrigues, A., Abeka, S. and Ogara, S. (2017), "Effectiveness of security controls on electronic health records", *International Journal of Scientific & Technology Research*, Vol. 6 No. 12, pp. 47-54.

Further reading

Archival Platform (2015), "State of archives: an analysis of South Africa's national archival system", available at: www.archivalplatform.org/news/entry/executive_summary/ (accessed 28 May 2023).

Katuu, S. (2015), "Managing records in South Africa's public sector – a review of literature", *Journal of the South African Society of Archivists*, Vol. 48, pp. 1-13.

Ngoepe, M. and Saurombe, A. (2016), "Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African development community", *Archives and Manuscripts*, Vol. 44 No. 1, pp. 24-41, doi: 10.1080/01576895.2015.1136225.

Salamntu, L.T.P. (2016), "Understanding achievements of benefits using enterprise content management (ECM) systems in public sector organisations", Master's Dissertation, University of Cape Town, Cape Town.

Ward, D.J. and Tao, E.Y. (2009), "Open-source software use in municipal government: is full immersion possible?", *Proceedings of the World Congress on Engineering and Computer Science*, 2: 20-22).

Corresponding author

Mahlatse Moses Shekgola can be contacted at: shekgmm@unisa.ac.za