Open Access Library Journal
2026, Volume 13, e15048
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Securing Archives and Records through the National Archives and Records Management System (NARMS): A Case of Botswana National Archives and Records Services (BNARS)

Nna Motlhasedi

Department of Information Science, University of South Africa, Pretoria, South Africa
Email: motlhny@unisa.ac.za

How to cite this paper: Motlhasedi, N. (2026) Securing Archives and Records through the National Archives and Records Management System (NARMS): A Case of Botswana National Archives and Records Services (BNARS). *Open Access Library Journal*, **13**: e15048.
https://doi.org/10.4236/oalib.1115048

Received: February 20, 2026
Accepted: April 21, 2026
Published: April 24, 2026

Abstract

The purpose of this study was to investigate the security of archives and records managed through the National Archives and Records Management System (NARMS) at Botswana National Archives and Records Services (BNARS). The study is a qualitative case study, where for sampling and the selection process of study respondents, the study adopted and used a purposive sampling method. Data collection was conducted through the use of observations, interviews and document analysis. While for data analysis, the study used a thematic analysis strategy. The study specifically sought to explore the different security measures of archives and records used through NARMS, and evaluate the effectiveness of the security measures for archives and records. The study's major finding is that the security of archives and records managed through NARMS is effectively executed by the authentication process and it is accompanied and enhanced by metadata management. However, the study further discovered that despite these strides, there is a failure to enhance archives and records security in the system because of a lack of access to the system's audit-trail logbook by archivists, nor can they monitor or examine it as archivists, despite their roles as systems administrators. As a result, user behaviour is not monitored, making it challenging to identify, look into, and ultimately demonstrate data or information violations and/or abuses. Based on these findings, the study recommends therefore that, BNARS consider giving records managers, archivists, or designated records managers and archivists who are systems administrators access to audit trail logbooks. Also, the study recommends that BNARS consider introducing the use of an encryption as a security protocol measure as a means of further ensuring optimum security of archives and records, as recommended by legislation. Being a case study, it has contextual and unique limitations and cannot

be generalised to other organizational contexts. The study contributes to the body of knowledge on the security of NARMS in archives and records management, specifically in the context of Botswana's archives and records management's governing body.

Subject Areas

Big Data Search and Mining

Keywords

Archives and Records Management, Records Management, Security, Digitization, National Archives and Records Management System (NARMS) at Botswana National Archives and Records Services (BNARS)

1. Introduction

Custodians of information recognise that records security is of utmost importance in ensuring that the integrity and reliability of information is met at all times. [1] citing the ISO-15489-1 corroborates this assertion by mentioning that there are four main characteristics of records: authenticity, reliability, integrity, and usability. Whereby, reliability, authenticity and integrity are ensured if state-of-the-art security measures are implemented in the electronic recordkeeping system and secure access control is reliably provided. "Records security can be defined as the degree of protection against danger, loss, and criminals. Records should be protected both from damage and unauthorized access. The method of security depends entirely on the storage method that has been adopted. Where computers are used, confidentiality can be maintained by giving a password to a document or file, which makes it difficult for another user who does not know the password to gain access to the file" [2].

According to [3], it is not to disprove a record's authenticity than it is to prove it is underpinned by several factors, such as the record's physical integrity, its chain of custody and the security of the repository in which it is stored, which is unquestionable. It is worth noting that in light of records security imperatives, it is therefore noted that throughout the records life cycle, the records and information management (RIM) experts in charge of organisational RIM initiatives handle matters including security, privacy, disaster recovery, evolving technologies, and mergers [4].

The Botswana National Archives and Records Services department was established in 1967 under the Ministry of Labour and Home Affairs as a unit. However, it was only in 1978 that the parliament of Botswana established the National Archives Act, BNA Act of 1978, which then therefore established officially the national archives as a preservation and conservation institution that provides access to the archives [5]. According to [6], in 1992, BNA changed its name to BNARS, and the mandate of the organization was expanded to include the provision of

leadership and professional competence in records management throughout the country's public sector. Furthermore, in 2007, the 1978 Act was revised to give BNARS the authority to coordinate the archives and records management function in Botswana, to preserve and make accessible records of enduring value. It also focused on ensuring that records that are 20 years and above are made open for public access and use [7]. The purpose of this study was to investigate the security of archives and records managed through the National Archives and Records Management System (NARMS) at Botswana National Archives and Records Services (BNARS). The specific objectives were to:

- Explore the different security measures for managing archives and records through NARMS at BNARS.
- Evaluate the effectiveness of security measures used for managing archives and records through NARMS at BNARS.

2. Problem Statement

An audit trail on activities undertaken within an archives and records management system is crucial to help uphold the security of the collection housed in such a system. NARMS is intended to enhance, uphold and ensure that records remain authentic, reliable, accessible, and protected from unauthorized access, alteration, or loss throughout the storage and existence. Thus, guaranteeing to uphold records confidentiality, integrity, and capacity to be made available at all times. However, NARMS despite its roll-out and implementation for use. An archivist, given the system administrator role, does not have access rights to monitor and examine the audit-trail logbook. Therefore, user actions are not tracked and are proving difficult to detect, investigate, and subsequently prove data or information breaches and/or misuse. Studies show that organizations with digital archives and records management systems or managing digital information should provide and maintain audit trails or any other methods that will demonstrate that records were effectively protected from unauthorised use, alteration or destruction. Without audit trails, the authenticity, reliability and accuracy of records are questionable because if records are not effectively managed and lack an audit trail, it will be difficult to detect fraudulent activities or any other act that may compromise the integrity of records [8] [9]. Hence, this study explored the security of archives and records managed through NARMS at BNARS. A feat that is fundamentally enhanced through the provision of a comprehensive audit trail.

3. Literature Review

3.1. Security Measures for Archives and Records Management Systems

Ensuring that records are available and are accurate to be used as a point of reference is centred around the security of records that are provided for the collection itself. Therefore, "a records management system results in a source of information about business activities that can support subsequent activities and business deci-

sions, as well as ensuring accountability to present and future stakeholders" [10]. [11] corroborates that by mentioning that electronic archives should feature security measures, pursuant to the provisions of the National Security Framework, which guarantee the integrity, authenticity, confidentiality, quality, protection and conservation of the records stored.

According to [12], archivists in digital curation for more technical aspects of security should develop at least a basic understanding of what it means to secure their digital collections. Where archivists undertake the process of protecting and ensuring records and archives security, as anchored on the legal and regulatory frameworks that guide on the process of doing so. A view carried by [13] who laments that governments need not focus on the increase on investment in information technology (IT) infrastructure and training skilled IT personnel, without developing clear regulatory frameworks and high security standards that are aimed at protecting sensitive information. In light of this, developed regions like Europe promulgated a law designated to the protection and security of information. In 2018, the General Data Protection Regulation (GDPR) was put into effect to help with compliance on data privacy and security. [14] mentions that organizations are required to handle data securely by implementing "appropriate technical and organizational measures". Where technical measures mean anything from requiring employees to use two-factor authentication on accounts where personal data are stored to contracting with cloud providers that use end-to-end encryption. While organizational measures are things such as staff trainings, adding a data privacy policy to employee handbooks, or limiting access to personal data to only those employees in the organization who need it.

While in Africa, several countries have enacted similar laws that are aimed at information security. South Africa has the Protection of Personal Information Act, Nigeria has the Data Protection Act, whereas Botswana has its own Data Protection Act of 2024. Essentially, these laws address security safeguards by emphasizing a requirement by organizations to implement technical and organizational measures to protect data from breaches. Therefore, measures to adopt and aid by ensuring the security of information, including being compliant with legal and regulatory frameworks, are but not limited to, access control, authentication and audit trails. With regards to access control as a security mechanism used to protect archives and records in an archives and records management system. [15] observes that the entire system should work on access control due to sensitive and confidential information stored in a system and therefore it should strictly prevent unauthorized access. [16] opines that there is a more compelling need to ensure the protection of privacy and limited access and control over files, and that the time for ad hoc decisions on access is over, both for the protection of the repository and for the protection of privacy rights of individuals, which archivists are ethically and legally bound to uphold. Access control imperatives are further mentioned in their study on medical electronic health records management systems by [17], who observed that access control is the primary mechanism for protecting

patients' privacy in electronic health records management systems.

Similarly, the authentication process helps uphold archives and records security through a thorough verification process to grant vetted and authorised individuals' access to the system and the archives and records collection itself. According to [18],

> "The preservation of confidentiality can also be ensured by ensuring information access to authorized persons. Identifying a set of persons who can access the information is the key to the process of authorization. Amongst the authorized persons, it is crucial to identify what portion of the information is available to whom and what actions (modification, addition, deletion, etc.) are available to be performed by an authorized person. This will ensure proper responsibility and accountability for all the users".

[12] opines that the "logical security" of collections involves an intangible process that identifies, authenticates, authorizes, protects, and provides access control measures over data and information. A crucial aspect to information integrity guarantees and assures improved and enhanced archives and records management systems security.

When there has been authentication, authorization and access granted into a system. User will in turn leave an audit trail that shows activities undertaken while using the system. [18] mentions that there is always a question of accountability, in case, something turns haywire. Thus, audit trail records are useful in such instances primarily because an audit trail logs all activities of addition, modification and deletion of entries in a system along with the date and time stamp in addition to access logs, authentication logs and any other related system activity logs. These are sentiments shared by [2] in their study, where they recommended that electronic records keeping systems should include adequate system controls, such as audit trails, and procedures for measuring the accuracy of data input and output.

3.2. Effective Security Measures for Archives and Records Management Systems (Access Controls, Authentication, Audit Trails)

Archives and records management systems ideally ensure that the collection housed into them is protected securely within them, and that their integrity is guaranteed at all times. However, in order to achieve this end. Several security protocol measures are incorporated within the system. Specifically with regards to access controls, authentication and audit trails, users are assured credible archives and records. Secure from compromised integrity due to unwarranted misuse and data breaches.

1) Access controls

Digital archives and records management systems adopt various methods to protect and secure information stored within them. Access controls are normally put in place to guard against intrusion and unauthorised access. [19] explains that the vital goal of any access control structure is to enforce a limit to access resources

and keep information from unauthorized access. Sentiments shared by [20] who laments that organizations have resorted to adopting digital information management systems such as enterprise content management (ECM) systems as they help to reduce risk by ensuring that contents are securely stored and made accessible only to authorized users. Through leading ECM solutions that have robust security features, such as access controls and audit trails. [20] further mentions that this ensures that sensitive information is protected and only accessible to authorized individuals, reducing the risk of data breaches and unauthorized access. While [21] remarks that in terms of security of records, measures such as access control should be implemented to prevent unauthorised access, alteration, concealment or destruction of records.

2) Authentication

In order to manage and succeed on providing an effective audit trail, users access the system, they are authenticated, authorised access and they eventually leave an audit trail regarding activities undertaken by themselves whilst using the system. Password-based access and log-in ID are the most popular and well-known authentication methods. In order to ensure that only selected individuals are granted access to the system. Systems administrators normally grant access via registration onto the system for future legitimate access and use. According to [22], reiterate this assertion that logging in, also known as sign-on, log-on, or log-on, is the process of identifying oneself to the system in order to gain access. Therefore, verifying the identity of any computer user or software trying to access the computer's services is the main purpose of a computer log-in process and ultimate authentication. The authority authentication service prevents unauthorized users from entering the system by setting user identity authentication and ensuring legal operations by legitimate users, and ensuring system security [23].

3) Audit trails

With all the necessary steps taken to ensure the security of information stored in the system. Inevitably, an audit trail is left behind by system users.

> "The chronological record of activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities—is inextricably linked to the provenance of a record, not just at the point of appraisal and accessioning, but from the record's point of creation, through its primary and active use by an individual or within an organization, and throughout its archival life" [24].

According to [25], an audit trail provides accountability, lowers fraud, demonstrates the actions of both individuals and the system, and allows for the reconstruction of transactions or occurrences. [26] argued that an audit trail, as a sequence of documents, computer files, and other records, subsequently shows how a transaction was handled in an organization from beginning to end. [27] reiterates this assertion by arguing that audit trails facilitate the process of determining accountability, effectiveness and integrity of an employee, a department, or even an organization by automatically capturing and storing all the actions that are

taken upon an electronic record, the user initiating and carrying out the action and the date and time of events. The authors [27] further explained that all types of information systems need to provide an audit trail feature for both audit purposes and security reasons.

4. Methodology

According to [28], a research methodology is defined as an approach or a unique and specific strategy that a researcher uses to conduct a study. This research adopted a case study design for its research methodology blueprint. Therefore, a case study research design was employed to identify issues and problems associated with the archives and records management security measures by NARMS at BNARS, which have not been extensively understudied yet. The target population for this study comprised of archivists and records managers employed in BNARS. The study employed a purposive sampling technique to select participants. According to [29], a purposeful sampling technique (also called judgment or subjective sampling) is the deliberate selection of participants based on their characteristics. In this technique, the researcher determines what information is needed and sets out to find people with knowledge or experience who can and will provide it [30].

When sampling using this method, the researcher identifies respondents who have characteristics that meet the study's needs. The sample was considered adequate because it included participants from all key roles involved in the system's operation and oversight, ensuring sufficient role coverage to capture relevant perspectives on the archives and records management processes on using NARMS. Therefore, through the use of this sampling technique, the researcher was able to collect qualitative responses, resulting in more precise and insightful research findings about NARMS security and protective capabilities from users of the system at BNARS. The total sample size for the study was 7 respondents, which comprised of 2 archivists, 4 records managers and 1 IT manager. Data was gathered using semi-structured interviews from selected study participants. This technique offered the researcher the freedom to explore any pertinent thoughts that arose throughout the interview. Furthermore, for data analysis, the study used the thematic analysis approach that was used to analyse qualitative data collected through interviews and document analysis. Thematic analysis is a qualitative research method used to systematically organise and analyze complex data sets. In this technique, narratives are captured in the account of data sets through the use of themes. Consequently, this technique was used to identify patterns and themes and interpret the data [31].

Specifically, the researcher obtained qualitative data through interviews, document analysis, and observations, which were analysed using thematic analysis. The researcher conducted the coding process, where interview transcripts and field notes were carefully reviewed to identify meaningful patterns related to the study objectives. An initial open coding approach was applied, in which segments of text were assigned descriptive codes representing key ideas, actions, or issues raised by

participants (P1 - P6) and the action officer (AO1).

After the initial coding, similar codes were grouped into broader categories, and these categories were further refined into themes that reflected recurring issues in the data, such as system security practices, access controls, audit logging, and records management procedures. The themes were developed inductively, meaning they emerged from the data rather than being imposed beforehand.

5. Findings

The study investigated the security of the National Archives and Records Management System (NARMS) at Botswana National Archives and Records Services Department. Therefore, the study findings are organised and presented in alignment with the research objectives, which are to explore the different security measures for managing archives and records through NARMS at BNARS and to evaluate the effectiveness of security measures used for managing archives and records through NARMS at BNARS. In order to get trustworthy responses from participants of the study, it is worth noting that the study used a code to anonymise participants as participant 1-6 represented as P1, P2 to P6 respectively and IT manager as action officer 1, represented as AO1.

5.1. Security Measures for Managing Archives and Records through NARMS at BNARS

Through observations, document analysis and interviews conducted at BNARS, the study established that NARMS has three (3) subsystems incorporated to make up the whole seamlessly functional ecosystem. These are the records management unit (RMU), the records centre (RC) and the archives administration (AA) subsystems, respectively. These subsystems have the following functions: the RMU subsystem registers, classifies and files records. It also transfers and destroys records or files. While the RC subsystem functions include file requests, file retrieval register, preservation list, destruction list, with the AA functions including accessioning of files, arrangement and description of archives and the preservation of archives.

In order to duly execute the functions listed for each subsystem without compromising on the accuracy and authenticity of the collection found in each subsystem. There is the security of the system that is in the form of access restrictions, which are imposed through the adoption and use of log-in details requirements, that facilitates privileges to access the system by users. Similarly, the findings showed that besides log-in details as a security protocol measure, metadata also is used by BNARS for the security of information. Different security measures are crucial as they enhance the protection of records and archives from unwarranted misuse, alterations and the compromise of the integrity of the information resource. These sentiments are shared by [32], who explain that security controls that organizations use play a significant role in developing trust by users of the system itself.

The study established that per descriptive metadata assigned to files that are either open, confidential, or top-secret files. The security of information within the collection is ensured by enforcing user rights restrictions based on the position of the system user, followed by their level of authority within the system itself. The study determined through observations the log-in requirements platform that users access in order to get authorisation into the system to view and use information stored within the system. Figure 1 shows the content manager authentication platform.

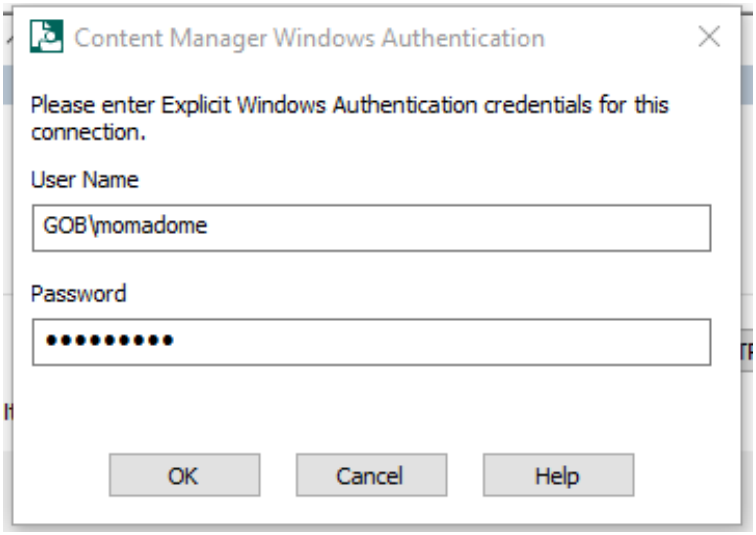

Figure 1. Content manager Windows authentication (Motlhasedi, 2024: p. 13) [33].

Figure 1 shows the first security protocol measure that NARMS has adopted and is using to control access by requiring log-in details to enable access rights. It is after logging into the system that, as noted by [33] users, through their usernames and passwords, they are allowed access into NARMS, whereby (through that metadata) they are filtered to access records according to their levels of authority, or they are granted access temporarily, informed by the same descriptive metadata.

The study through interviews found that the use of log-in credentials was appreciated by users and considered an ideal method to adopt in protecting information kept within the system. The researcher posed the question,

What are all the security measures adopted for use found in NARMS?

P1 answered,

"I am not sure about all of them, but I do know there are log-in detail requirements, and that the system has an audit trail left by users".

P4 replied,

"Log-in details and metadata management. It is through metadata that files are categorised as either open, confidential, secret or top-secret. Therefore, depending on the level of authority of users of the system, access rights are

granted to users to files. Also, where access is denied, users can request for it, and they can be given temporary access to files that they are not necessarily always accessing".

While AO1 opined that,

"The system is still at a piloting phase, it is not fully implemented. It is a 3-phase system that is operating at a 1/3rd of its operational phase capacity. Its security measures are log-in details requirements, an audit trail that produces a report."

To further establish familiarity with identified security measures in place by BNARS, the researcher posed another question by asking,

What is the method used by NARMS to provide security to archives and records, and in your opinion, is this process sufficient in upholding good security to the collection?

In answering the question, P1 mentioned that,

"The system has enhanced security that uses log-in details requirements to have access into the archives and records".

P2 stated that,

"There is the initial access point of populating the user's log-in details, a process that filters authorised from unauthorised users of the system. Also, NARMS has an audit trail, which I don't remember going through it not once. Therefore, I don't even know if it is functional or not".

While P3 briefly mentioned that,

"All I know is that we have to use log-in details for authentication and authorisation into the system. I understand it to help with security".

However, the study further established through interviews that there is no specific binding regulatory framework that the system is guided by, except for the statement of user requirements (SOUR) document. Therefore, the security of the collection found in NARMS is largely informed by the specifications determined during the procurement phase of the system. Document analysis of the SOUR framework established that those who access records in the system will largely be regulated by the officer's job title and organizational unit affiliation.

5.2. Effective Security Measures for Managing Archives and Records through NARMS at BNARS

It is imperative to setup effective means of protecting and securing archives and records, especially those found in digital systems. Accordingly, [4] reiterated this assertion by arguing that solutions established for digital systems have robust security features effective to granting security and sureties on the validity and accuracy of the information that is stored inside them. Therefore, regarding the effec-

tiveness of NARMS at BNARS. The study established through interviews that there is still room for improvement and the possible betterment of security provided by NARMS. The researcher asked participants,

> "What security measures are ideal and effective to improve NARMS for BNARS?".

P1 stated that, "*NARMS has audit trail capability, but as the administrator I have never accessed the audit trail logbook and I don't know if the IT administrator is the only one that has its access rights or not*".

P3 raised concerns that, "*the system constantly goes offline and there are no guarantees regarding back up and disaster recovery capabilities*".

P4 explained that, "*technology keeps evolving and needs a proactive approach to deal with threats and risks associated with it. BNARS should liaise with relevant government bodies to improve NARMS security by including data encryptions*".

Through document analysis, specifically the SOUR document. The study found that NARMS was intended to have capabilities of security, such as encryptions, digital signatures and audit trails, which can be produced by both IT systems administrators, records managers and archivists.

Similarly, the researcher posed another question to respondents that,

> "Are the methods adopted for NARMS security provision effective to protect both archives and records found in the system?".

This question had a varying level of trust to it, it was discovered that AO1 viewed the system as secure and effective on the delivery of its mandate. The respondents identified trained personnel, log-in details requirements and its piloting internal phase as a crucial element that guards against information losses, or their state being compromised. AO1 mentioned that, since BNARS personnel is trained and appreciates the importance of archives, records and information. They are the first line of protection, as they are doing what is ethically right as per archives and records management standards. The respondent also highlighted that with the use of log-in details, it is effective to filter access and if there are breaches. As the system's administrator, it is easy for the IT department to track such breaches and ensure access restrictions aren't compromised any further. However, the respondent emphasized a need to adopting encryptions and digital signatures to strengthen the overall security of the system beyond what is already in use.

While other respondents explained that,

P5 "Without ever accessing audit trail logbooks as an archivist, I cannot confidently endorse the system as I do not know if there are data breaches. As I cannot investigate and establish any misuse activities".

Observations on the system itself established that audit trails through the active audit field provide users with an opportunity to determine access and usage of records found in the system.

Through document analysis, specifically the BNARS Act of 2007 and the Data

Protection Act of 2024. The researcher determined that authentication controls support the Data Protection Act's requirement for organisations to implement appropriate technical measures that prevent unauthorized access to personal information. Access restrictions and role-based permissions align with the Act's principles of confidentiality and controlled processing of personal data, ensuring that only authorised personnel can view or manage sensitive records. Audit trails contribute to accountability and traceability obligations by maintaining logs of system activities, which enable monitoring, investigation of potential breaches, and verification of compliance with records management policies. Finally, encryption and digital signatures support the protection of data integrity and confidentiality during storage and transmission, while also reinforcing archival requirements to maintain the authenticity and reliability of records as mandated by BNARS regulatory frameworks.

Together, these controls demonstrate how the system's security mechanisms operationalise legal requirements for data protection, record integrity, and accountability, thereby helping the organisation align its archives and records management practices with both national data protection legislation and archival governance standards.

6. Conclusions and Recommendations

The study concludes that the system is suitable to aid in improved archives and records management as intended. It is not fully implemented for full usage, as only the RC subsystem is functional. However, it has proven to be effective in the management of records and therefore, the department will have an effective system altogether when it commences with the remaining subsystems. For recommendations:

- The study recommends that access to an audit trail logbook should be granted to records managers, archivists or designated records managers and archivists who are systems administrators, to ensure that security measures go beyond the use of passwords to log into the system, to ensure that housed archives and records collections in the system can be said to be trustworthy, reliable and authentic, as it will be protected from misuse and unauthorised alterations. Due to the ease in tracking what the archives and records are subjected to within the system itself. Information about the controls that were applied to a record and when they were applied should be recorded in the record's process metadata (ISO 15489-1 2016).
- The study further recommends that alternative measures be adopted to enhance the protection and security of archives and records in the system, in the form of data encryption capabilities, digital signatures, as initially intended and delineated in the SOUR document.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] McLeod, J. (2005) Electronic Records: A Workbook for Archivists. ICA Study 16. International Council on Archives. *Records Management Journal*, **15**, 1-104. https://doi.org/10.1108/rmj.2005.28115cae.003

[2] Aramide, O.K., Ajibola, R.E., Olatunji, O.S. and Oduroye, P. (2020) Improving Records Management and Security for Successful Business Performance: The Role of New Media. *Library Philosophy and Practice* (*E-Journal*). https://digitalcommons.unl.edu/libphilprac/3734

[3] Seymour, J. (2017) The Modern Records Management Program: An Overview of Electronic Records Management Standards. *Bulletin of the Association for Information Science and Technology*, **43**, 35-39. https://doi.org/10.1002/bul2.2017.1720430212

[4] Nyampong, S.A. (2015) Electronic Records Management in National Development: A Case Study in Ghana Immigration Service. *European Journal of Business and Management*, **7**, 120-144.

[5] Phologolo, A., Oladokun, O. and Mosweu, T. (2024) Managing Heritage: A Study of Archival Collections Handling Practices at Botswana National Archives and Records Services. *African Journal of Library, Archives & Information Science*, **34**, 173-188.

[6] Masibi, T.J., Mnjama, N. and Sebina, P.M.I. (2023) Archival Silences within the National Archival Documentary Heritage Institutions of Botswana. *African Journal of Library, Archives and Information Science*, **33**, 245-257. https://doi.org/10.4314/ajlais.v33i2.9

[7] Moloi, J. (2021) Long-Term Preservation for Access of Audio-Visual Archives at Botswana National Archives (Bnars). In: Chisita, C.T., Enakrire, R.T., Durodolu, O.O., Tsabedze, V.W. and Ngoaketsi, J.M., Eds., *Handbook of Research on Records and Information Management Strategies for Enhanced Knowledge Coordination*, IGI Global, 92-109. https://doi.org/10.4018/978-1-7998-6618-3.ch006

[8] Mosweu, T.L. and Kenosi, L. (2018) Implementation of the Court Records Management System in the Delivery of Justice at the Gaborone Magisterial District, Botswana. *Records Management Journal*, **28**, 234-251. https://doi.org/10.1108/rmj-11-2017-0033

[9] Rakemane, D. and Serema, B.C. (2018) Electronic Records Management Practices at the Companies and Intellectual Property Authority in Gaborone, Botswana. *Journal of the South African Society of Archivists*, **51**, 148-169.

[10] International Standard ISO 15489-1 (2001) Information and Documentation—Records Management—Part 1: Concepts and Principles. http://www.wgarm.net/ccarm/docs-repository/doc/doc402817.PDF

[11] Casadesús de Mingo, A. and Cerrillo-i-Martínez, A. (2018) Improving Records Management to Promote Transparency and Prevent Corruption. *International Journal of Information Management*, **38**, 256-261. https://doi.org/10.1016/j.ijinfomgt.2017.09.005

[12] Donaldson, D.R. and Bell, L. (2018) Security, Archivists, and Digital Collections. *Journal of Archival Organization*, **15**, 1-19. https://doi.org/10.1080/15332748.2019.1609311

[13] Makmur, S. (2023) Implementation of Archives Digitization Policy as a Form of Implementation of an Electronic-Based Government System. *Journal of Social Research*, **2**, 1847-1852. https://doi.org/10.55324/josr.v2i6.921

[14] Wolford, B. (2025) What Is GDPR, the EU's New Data Protection Law? GDPR.EU. https://gdpr.eu/what-is-gdpr/

[15] Jakhar, A.K., Singh, M., Sharma, R., Viriyasitavat, W., Dhiman, G. and Goel, S. (2024) A Blockchain-Based Privacy-Preserving and Access-Control Framework for Electronic Health Records Management. *Multimedia Tools and Applications*, **83**, 84195-84229. https://doi.org/10.1007/s11042-024-18827-3

[16] Galloway, P. (2021) Providing Restricted Access to Mental Health Archives within Government Archives: The Subject Stakeholder. *The American Archivist*, **84**, 165-188. https://doi.org/10.17723/0360-9081-84.1.165

[17] Jayabalan, M. and O'Daniel, T. (2016) Access Control and Privilege Management in Electronic Health Record: A Systematic Literature Review. *Journal of Medical Systems*, **40**, Article No. 261. https://doi.org/10.1007/s10916-016-0589-z

[18] Gopal, D.G. and Haran, U.H. (2019) Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions. *Security and Privacy of Electronic Healthcare Records*, 249-266.

[19] Ravinder Reddy, B. and Anil Kumar, A. (2019) Survey on Access Control Mechanisms in Cloud Environments. In: Chillarige, R., Distefano, S. and Rawat, S., Eds., *International Conference on Advances in Computational Intelligence and Informatics*, Springer, 141-149. https://doi.org/10.1007/978-981-15-3338-9_18

[20] Chaterera-Zambuko, F. (2023) Enterprise Content Management System Implementation: Insights from the National Library and Archives of UAE. *Information Development*, **42**, 179-193. https://doi.org/10.1177/02666669231211539

[21] Mosweu, T. (2019) The Good, the Bad and the Ugly: Social Media Prospects and Perils for Records Management. *ESARBICA Journal: Journal of the Eastern and Southern Africa Regional Branch of the International Council on Archives*, **38**, 45-62. https://doi.org/10.4314/esarjo.v38i1.3

[22] Shoeb, Z.H. and Sobhan, M.A. (2010) Authentication and Authorization: Security Issues for Institutional Digital Repositories. *Library Philosophy and Practice* (*E-Journal*).

[23] Lv, Z. and Shi, H. (2020) The Exploring on University Archives Management System Based on Information System. *Journal of Physics: Conference Series*, **1550**, Article ID: 032017. https://doi.org/10.1088/1742-6596/1550/3/032017

[24] Noonan, D. (2016) Capturing Audit Trail Data. Theory: Authenticity and Audit. In: Bantin, P.C., Ed., *Building Trustworthy Digital Repositories: Theory and Implementation*, Rowman & Littlefield, 169, 171.

[25] Kupec, V., Sieber, J. and Baycan, I.O. (2022) Documentation Management and the Audit Trail in Public Administration. *Slovak Journal of Public Policy and Public Administration*, **9**, 97-113. https://doi.org/10.34135/sjpppa.220908

[26] Law, J. and Smullen, J. (2008) A Dictionary of Finance and Banking. Oxford University Press.

[27] Ngoepe, M. and Ngulube, P. (2016) A Framework to Embed Records Management into the Auditing Process in the Public Sector in South Africa. *Information Development*, **32**, 890-903. https://doi.org/10.1177/0266666915573037

[28] Jansen, D. and Warren, K. (2020) What Is Research Methodology? https://gradcoach.com/what-is-research-methodology/

[29] Etikan, I., Musa, S.A. and Alkassim, R.S. (2016) Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, **5**, 1-4. https://doi.org/10.11648/j.ajtas.20160501.11

[30] Bernard, H.R. (2002) Research Methods in Anthropology: Qualitative and Quantitative methods. 3rd Edition, AltaMira Press.

[31] Braun, V. and Clarke, V. (2012) Thematic Analysis. In: Cooper, H., Ed., *The Handbook of Research Methods in Psychology*, American Psychological Association, 57-71.

[32] Thabakgolo, M. and Nsibirwa, Z. (2023) Trust in Electronic Records-Keeping Systems among Selected Botswana Parastatals. *Mousaion*: *South African Journal of Information Studies*, **41**, 18 p. https://doi.org/10.25159/2663-659x/12982

[33] Motlhasedi, N. (2024) An Assessment Study of the National Archives and Records Management System (NARMS) at Botswana National Archives and Records Services (BNARS). *Mousaion*: *South African Journal of Information Studies*, **43**, 20 p. https://doi.org/10.25159/2663-659x/14068