SCHOOL OF LIBRARY, ARCHIVES AND DOCUMENTATION STUDIES(SLADS)-BAGAMOYO

A RESEARCH REPORT ON:

AN ASSESSMENT OF THE USE OF DIGITAL RECORD MANAGEMENT ON DATA INTEGRITY AND SECURITY: A CASE STUDY AT DAR ES SALAAM INSTITUTE OF TECHNOLOGY (D.I.T)

BY

RAMADHAN AHMED MBWILO

A Research Report Submitted to the School of Library, Archives and Documentation Studies in Partial Fulfilment of the Requirements for the Award of Ordinary Diploma in Records and Archives Management

August,2026

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CERTIFICATION

The undersigned certifies that he has read and hereby recommends for acceptance by the School of Library, Archives and Documentation Studies (SLADS), Tanzania Library Services Board (TLSB), a research report titled “An Assessment of the Use of Digital Record Management on Data Integrity and Security: A Case Study at Dar es Salaam Institute of Technology (D.I.T)”, in partial fulfilment of the requirements for the award of the Ordinary Diploma in Records and Archives Management Studies of the Tanzania Library Services Board (TLSB).

.

Supervisor's Name: MR. LYIMO

Signature: _____

Date: _____

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

DECLARATION AND COPYRIGHT

I, Ramadhan Ahmed Mbwilo hereby declare that this research report is my own original work and it has not been presented, and will not be presented, to any other institution or university for a similar or any other award of a degree or diploma. All sources of information used in this report have been duly acknowledged by means of references.

Student's Signature: _____

Date: _____

COPYRIGHT

This research report is copyright material protected under the Berne Convention, the Copyright and Neighbouring Rights Act (Cap. 218 R.E. 2019), and other applicable international and national laws on intellectual property. It may not be reproduced by any means, in full or in part, except for short extracts in fair dealing for research or private study, critical scholarly review, or discourse with acknowledgement, without prior written permission of the School of Library, Archives and Documentation Studies (SLADS), Tanzania Library Services Board (TLSB), on behalf of the author.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

ACKNOWLEDGEMENT

First and foremost, I thank the Almighty God for the gift of life, good health, strength and wisdom throughout the period of undertaking this research.

I wish to express my sincere and heartfelt gratitude to my supervisor, Mr. Lymo, for his invaluable guidance, patience, constructive criticism and tireless supervision from the initial to the final stages of this research report. His encouragement and professional insight greatly shaped the quality of this work.

Special appreciation goes to Mr. Mbwilo and Mr. Kibasa for their support, advice and encouragement, which contributed significantly to the successful completion of this study.

I am also grateful to the management and staff of the Dar es Salaam Institute of Technology (DIT) for allowing me to conduct this study within their institution and for their cooperation during data collection.

My sincere thanks also go to my classmates, for their moral support, teamwork and constructive discussions throughout this journey, as well as to my family, for their patience, love and unwavering support throughout my studies.

Lastly, I extend my appreciation to everyone, named and unnamed, who contributed in one way or another towards the successful completion of this research report. May the Almighty God bless you all.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

DEDICATION

This work is dedicated to my beloved parents and family, for their endless love, prayers, sacrifice and unwavering support throughout my studies. It is further dedicated to the Almighty God, for His grace, protection and guidance that has brought me this far; to my friends, for their encouragement and companionship; to my lecturers, for the knowledge and skills they generously imparted; and to all professionals in the field of records and archives management, whose dedication to safeguarding the integrity, security and accessibility of information continues to inspire this study.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

LIST OF ABBREVIATIONS AND ACRONYMS

AI	- Artificial Intelligence
BFSI	- Banking, Financial Services, and Insurance
DIT / D.I.T	- Dar es Salaam Institute of Technology
DRM	- Digital Records Management
DRMS	- Digital Records Management System
EDMS	- Electronic Document Management System
EDRMS	- Electronic Document and Records Management System(s)
ERMS	- Electronic Records Management System
ICA	- International Council on Archives
ICT	- Information and Communication Technology
IRMT	- International Records Management Trust
ISO	- International Organization for Standardization
MFA	- Multi-Factor Authentication
NARA	- National Archives and Records Administration
NCIRT	- National Computer Incident Response Team
OAIS	- Open Archival Information System
ODPC	- Office of the Data Protection Commissioner
PDPA	- Personal Data Protection Act
RBAC	- Role-Based Access Control
RMFA	- Records Management Foundation for Africa
SLADS	- School of Library, Archives and Documentation Studies
SPSS	- Statistical Product and Service Solutions
SQL	- Structured Query Language
URT	- United Republic of Tanzania
TLSB	- Tanzania Library Services Board

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

ABSTRACT

This study assessed the use of digital record management on data integrity and security, using the Dar es Salaam Institute of Technology (DIT) as a case study. The general objective of the study was to assess the use of digital record management practices in enhancing data integrity and security, guided by four specific objectives: to assess the existing digital record management practices and technologies at DIT; to evaluate the technical controls and policy measures in place to safeguard data integrity and security; to identify the challenges affecting data integrity and security within the current system; and to identify measures for improving data integrity and security.

The study adopted a mixed-methods approach, combining questionnaires and interviews within a single case study design, to obtain detailed information from 50 respondents comprising registry staff, records officers, and other users of DIT records.

The findings revealed that DIT still relies heavily on a hybrid record-keeping system, combining paper-based and digital records, with only a small proportion of respondents reporting the use of a fully digital system. While access control and data backup were found to be functioning reasonably well, audit trails and encryption were identified as weak areas, limiting DIT's ability to demonstrate who accessed or altered a given record. The major challenges affecting data integrity and security included poor staff training, the persistence of the hybrid system, poor network connectivity, cyber threats, a low ICT budget, and incomplete policies, alongside the risk of insider threats arising from unrestricted access to records. Respondents recommended staff training, full digitization of records, stronger security policies, increased ICT budgetary allocation, and the adoption of emerging technologies such as blockchain and artificial intelligence as key measures for improvement.

The study concluded that DIT requires a clear and comprehensive plan to strengthen its digital record management system, one that emphasizes staff training, stronger policies aligned with international standards such as ISO 15489 and ISO 27001:2022, and greater

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

investment in ICT infrastructure, in order to fully safeguard data integrity and security. The study recommends that DIT institutionalize regular staff training, adopt a phased transition to a fully digital system, formalize data security policies in line with recognized international standards, and invest in more reliable ICT infrastructure, including automated backup systems.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

TABLE OF CONTENTS

CERTIFICATION I
DECLARATION AND COPYRIGHT II
COPYRIGHT II
LIST OF TABLES XI
LIST OF FIGURES XII
INTRODUCTION AND BACKGROUND TO THE STUDY 1
1.0 Introduction 1
1.1 Background to the Problem 1
1.2 Statement of the Problem 6
1.3 General Objective 7
1.4 Specific Objectives 7
1.5 Research Questions 7
1.6 Significance of the Study 7
1.7 Scope of the Study 8
1.8 Limitations of the Study 9
1.8 Definition of Key Terms 10
LITERATURE REVIEW 12
2.0 Introduction 12
2.1 Existing Digital Records Management Practices and Technologies 13
2.2 Evaluation of Technical Controls and Policy Measures for Safe Guarding Data Integrity and Security 14
2.3 Challenges Affecting Data Integrity and Security in Current Systems 16
2.8 Measures for Improving Data Integrity and Security 17
2.9 Conceptual Framework 19
2.10 Research Gap 19
RESEARCH METHODOLOGY 21
3.0 Introduction 21
3.1 Research Design 21
3.2 Research Approach 21
3.3 Area of the Study 22

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

3.4 Population 23
3.5 Sample Size 23
3.6 Sampling Procedures 23
3.7 Data Collection Method 24
3.8 Data Analysis and Processing 26
3.9 Pilot Study 26
3.9 Validity and Reliability 26
3.10 Research Ethics 27
3.11 Chapter Summary 27
DATA PRESENTATION, ANALYSIS AND DISCUSSION 28
4.0 Introduction 28
4.1 Demographic Information of Participants 28
4.1.1 Gender of Participants 28
4.1.2 Education Level of Participants 30
4.1.3 Age Group of Participants 32
4.2 Existing Digital Record Management Practices and Technologies at Dit 33
4.2.1 How Participants Access Digital Records 33
4.2.2 Ease of Locating Record Materials 35
4.2.3 Relevance of Information Retrieved 37
4.2.4 Interview Findings on Current Practices 38
4.3 Technical Controls and Policies for Protecting Data Integrity and Security 39
4.3.1 Effectiveness of Technical Controls 39
4.3.2 Interview Findings: Views of Records Officers 40
4.3.3 Satisfaction with the Digital Record System 41
4.3.4 Interview Findings on Technical Controls 42
4.4 Challenges Affecting Data Integrity and Security in the Current System 42
4.4.1 Main Challenges Identified 42
4.4.2 Challenges Faced When Accessing Digital Records 43
4.4.3 Interview Findings on Challenges 44
4.5 Measures to Improve Data Integrity and Security 45

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

4.5.1 Participants' Recommendations 45
4.5.2 Interview Views on Improvement Measures 46
4.6 Chapter Summary 47
CHAPTER FIVE 48
SUMMARY, CONCLUSION AND RECOMMENDATIONS 48
5.0 Introduction 48
5.1 Summary of Findings 48
5.1.1 Objective One: Digital Record Management Practices and Technologies 48
5.1.2 Objective Two: Technical Controls and Policies 48
5.1.3 Objective Three: Challenges Affecting Data Integrity and Security 48
5.1.4 Objective Four: Measures to Improve the System 49
5.2 Conclusion 49
5.3 Recommendations 50
5.3.1 Recommendations for DIT 50
5.3.2 Recommendations for Government and Policy Makers 50
5.3.3 Recommendations for Further Research 51
5.4 Contribution of the Study 51
5.5 Chapter Summary 52
5.6 Areas for Further Study 52
REFERENCES 59
DETAILEDRESEARCHBUDGET 64
APPENDIXII 65
TIMESCHEDULE 65
APPENDIXIII 66
QUESTIONNAIRES GUID FOR REGISTRY STAFF RESIDENTS 66
APPENDIXIV 69
INTERVIEW GUIDE QUESTIONS FOR RECORD OFFICERS 69

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

LIST OF TABLES

Table 4.1: Gender of Participants (n=50) 26

Table 4.2: Education Level of Participants (n=50).....27

Table 4.3: Age Groups of Participants (n=50).....29

Table 4.4: Show Participants Access Digital Records (n=50).....31

Table 4.5: Ease of Locating Record Materials (n=50).....32

Table 4.6: Relevance of Information Retrieved from the Digital Record System (n=50).34

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

LIST OF FIGURES

Figure 4.1: Gender of Participants (n=50) 27

Figure 4.2: Education Level of Participants (n=50) 28

Figure 4.3: Age Groups of Participants (n=50) 30

Figure 4.4: How Participants Access Digital Records (n=50) 32

Figure 4.5: Ease of Locating Record Materials (n=50) 33

Figure 4.6: Relevance of Information Retrieved from the Digital Record System 35

Figure 4.8: Satisfaction with the Digital Record System (n=50) 38

Figure 4.7: How Well Technical Controls Are Working at DIT (n=50) 36

Figure 4.9: Challenges Affecting Data Integrity and Security (n=50) 39

Figure 4.10: Challenges Faced When Accessing Digital Records (n=50) 41

Figure 4.11: Measures Recommended to Improve the System (n=50) 43

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CHAPTER ONE

INTRODUCTION AND BACKGROUND TO THE STUDY

1.0 Introduction

This chapter presented the background to the study, statement of the problem, general objective, specific objectives, and research questions, significance of the study, the scope of the study, limitation of the study, and the definitions of the key terms. This study specifically focused on Dar es Salaam Institute of Technology (DIT), a prominent higher learning institution in Tanzania that had increasingly adopted digital record management systems in its administrative and academic operations. DIT served as an appropriate case study due to its transition from paper-based to hybrid and digital recordkeeping systems, presenting an opportunity to examine data integrity and security challenges in a real-world educational context.

1.1 Background to the Problem

In the modern digital era, organizations across sectors had increasingly adopted digital record management systems to support efficient information capture, storage, retrieval, and long-term preservation. Digital record management had become a critical component of organizational operations in the 21st century, fundamentally transforming how institutions stored, accessed, and protected information. The transition from paper-based to digital systems had been accelerated by technological advancements, regulatory requirements, and the need for operational efficiency (Katuu, 2021). Organizations across sectors, including healthcare, finance, government, and education, relied heavily on electronic records management systems to maintain business continuity and competitive advantage.

GLOBALLY, organizations had increasingly adopted digital records management systems (DRMS) to improve efficiency, accessibility, and decision-making. Digital records management referred to the systematic control of electronic records throughout their lifecycle, including creation, storage, retrieval, and disposal (ISO 15489-1, 2020). This exponential growth in data generation had necessitated sophisticated digital record management systems to ensure data integrity and security. The first half of 2024

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

witnessed over 6 billion records breached across 2,741 sites with the average cost of a data breach reaching $4.88 million, representing a 10% increase from the previous year (Corodata Team, 2025; DPO Consulting, 2025). Digital record management had evolved from simple electronic filing systems to complex ecosystems incorporating artificial intelligence, block chain technology, and advanced encryption protocols. Organizations across healthcare, legal, financial, and government sectors had increasingly implemented electronic document management systems (EDMS) to centralize document storage, enhance accessibility, and strengthen security measures (Augusta Data Storage, 2024). The adoption of cloud-based solutions had reached projected rates of 90% among businesses by 2025, fundamentally reshaping how organizations managed and protected their digital assets (Crudu & MoldStud Research Team, 2025).

However, this digital transformation had introduced significant challenges related to data integrity and security. Data integrity ensured that information remained accurate, complete, and unaltered, while data security protected records from unauthorized access, loss, or cyberattacks (Alhassan & Adjei, 2022). Studies in developed countries showed that effective digital records management enhanced transparency, accountability, and service delivery, but poor implementation led to data breaches and loss of trust (Katuu, 2021). Emerging technologies such as block chain had gained traction for their ability to provide immutable record-keeping and enhanced transparency. Block chain solutions enabled organizations to track document handling through digital ledgers, preventing unauthorized alterations and ensuring data authenticity (Corodata Team, 2025; Learn & Work Ecosystem Library, 2025). The regulatory environment had also hardened significantly, with frameworks like the European Union's AI Act imposing fines up to €35 million or 7% of global annual revenue for non-compliance, emphasizing the critical intersection of digital record management, data integrity, and security (G+D Spotlight, 2025).

AFRICA, formal adoption of digital records management began in the early 2000s, driven by e-government initiatives and administrative reforms (Asogwa & Ezema, 2021). Countries such as South Africa, Kenya, and Rwanda had introduced electronic document and records management systems to improve public service delivery. Although progress

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

had been made, many African organizations still operated hybrid systems, which compromised effective digital records management and data protection. Africa's data protection and digital transformation landscape witnessed remarkable developments in 2024, reflecting the continent's commitment to establishing robust frameworks for digital record management and data security. The African Union's Data Policy Framework, adopted in 2022, had guided member states in building national systems aligned with continental principles, while the Malabo Convention on Cyber Security and Personal Data Protection achieved official enforcement on June 8, 2023, after ratification by multiple countries (Tech Hive Advisory, 2024; ICT Works, 2024). During 2024, significant legislative progress occurred across the continent. Cameroon, Ethiopia, and Malawi enacted new data protection laws, while Botswana amended its existing legislation. Several countries, including Congo, Democratic Republic of Congo, Somalia, and Togo, established their Data Protection Authorities (DPAs), while Tanzania officially launched its Personal Data Protection Commission (Tech Hive Advisory, 2024). These developments demonstrated Africa's proactive approach to addressing data governance challenges in the digital era.

However, African institutions faced persistent challenges including inadequate ICT infrastructure, limited professional skills, weak policy frameworks, and increasing cybersecurity threats (Ngoepe & Saurombe, 2022). Interpol (2023) reported a rise in cybercrime across African public institutions, affecting the integrity and security of digital records. The cybersecurity market in Africa had experienced substantial growth, with market size valued at USD 4.84 billion in 2024 and projected to reach USD 25.79 billion by 2033, growing at a CAGR of 20.43% (Market Data Forecast, 2025). This growth was driven by digital transformation initiatives, rising cyber threats, government investments, and increased cloud adoption across the continent. The Banking, Financial Services, and Insurance (BFSI) sector commanded the largest share of cybersecurity investments, holding an estimated 26.4% market share in 2024, reflecting the sector's high vulnerability to cyber threats due to extensive digital footprints and large transaction volumes (Market Data Forecast, 2025). African governments had prioritized cyber resilience, with countries like Ghana launching nationwide initiatives to protect e-governance platforms through threat intelligence centers and cyber emergency response

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

teams. Kenya's National Computer Incident Response Team (NCIRT) reported significant increases in cyberattacks targeting public institutions, leading to enhanced budget allocations for cyber defense (Market Data Forecast, 2025). Financial institutions in East Africa allocated nearly 20% of their IT budgets to cybersecurity enhancements in 2023, including investments in encryption, multi-factor authentication, and behavioral analytics tools (Market Data Forecast, 2025). The Records Management Foundation for Africa (RMFA) had been instrumental in promoting best practices in digital record management across the continent. The organization had conducted conferences in multiple African cities, including Dar es Salaam, Nairobi, Kampala, Lusaka, and Harare, focusing on leveraging technology in e-records management, library services, and e-governance (RMFA, 2024). The emphasis on cybersecurity in e-records management, data privacy protection, and building sustainable infrastructure for electronic libraries reflected the continent's holistic approach to digital transformation (RMFA, 2024). Enforcement of data protection laws had intensified across Africa. Kenya's Office of the Data Protection Commissioner (ODPC) issued a record number of fines and sanctions during 2024, while South Africa's Information Regulator imposed a ZAR 5 million (USD 279,000) fine on the Department of Justice and Constitutional Development for violations including failure to renew licenses for critical cybersecurity components (ICT Works, 2024). Angola's National Data Protection Authority fined Africell $150,000 for processing customer personal data without prior authorization (ICT Works, 2024).

TANZANIA, digital records management officially started gaining momentum after the introduction of the National ICT Policy in 2003, later revised in 2016. The government had further strengthened digital governance through the establishment of the e-Government Agency (eGA) in 2012 (URT, 2023). Public institutions began implementing electronic recordkeeping systems in the mid-2000s to support service delivery, transparency, and accountability. Despite these initiatives, studies showed that many Tanzanian organizations lacked standardized DRM policies, skilled personnel, and adequate security controls (Mnjama & Wamukoya, 2022). The enactment of the Personal Data Protection Act (PDPA) 2023 represented a landmark legislative achievement, affirming privacy as both a constitutional and human right within Tanzania's digital environment (Ernest, 2025). The PDPA incorporated globally recognized principles of

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

lawfulness, fairness, and accountability, positioning Tanzania among African countries with comprehensive data protection frameworks.

However, the Act's implementation faced challenges including vague statutory provisions, overlapping institutional mandates, weak regulatory capacity, and limited public awareness (Ernest, 2025). Tanzania's digital transformation was anchored on the Tanzania Technology Stack, which formed the foundation for the country's 10-year Digital Economy Strategy Framework launched on July 29, 2024, by President Samia Suluhu Hassan. This technology stack included key platforms such as Jamii Namba (digital ID with over 25 million citizens registered), Jamii Malipo (digital payments), and Jamii Data Shirikishi (Jamii X-Change for seamless data sharing across government services) (DPI Africa, 2024). These platforms operated with four essential sublayers consent, paperless, cashless, and presence less, addressing challenges in service delivery, including high transaction costs and limited access to financial services. The director of ICT Systems Development at the Ministry of Communication and Information Technology emphasized that data had become a national asset that could fuel innovation and economic growth if well managed. The initiative was linked to Tanzania's ambition to not only ensure security but also create value from data, including space data, through strong policies, regulations, and standards (The Citizen, 2025). Tanzania's efforts positioned the country to potentially inspire other East African Community member states, many of which were grappling with data localization and cybersecurity challenges.

The transition to digital record management was particularly evident in public sector institutions and e-government initiatives. Electronic office systems had been introduced to improve transparency, efficiency, and accountability in service delivery. While such systems had enhanced access and control of records, challenges in ensuring security and confidentiality persisted due to organizational capacity gaps, limited ICT infrastructure, and the continued use of hybrid (paper + digital) systems (Kashaija, 2023). Tanzania's efforts to address data integrity concerns extended to broader issues like digital evidence management and cybersecurity. At the sectoral level, studies of e-records guidance tools in Tanzanian institutions highlighted that aspects such as user awareness, procedural compliance, and regulatory clarity significantly influenced digital record sharing

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

practices, with implications for secure and reliable information handling (Chang'a & Mwilongo, 2022). Dar es Salaam Institute of Technology (DIT) was one of the institutions that had started using digital systems to manage its records. DIT handled many types of records, including student academic records, staff files, financial documents, and administrative papers. As DIT moved towards more digital systems, it was important to understand how these systems affected data integrity and security. This study looked at this issue at DIT.

1.2 Statement of the Problem

Despite significant assessment in digital infrastructure and the enactment of the Personal Data Protection Act 2023, Tanzania faced critical challenges in implementing effective digital record management systems that ensured data integrity and security. Dar es Salaam Institute of Technology (DIT), like many higher learning institutions in Tanzania, had embraced digital transformation in its records management practices. The institution managed various types of records including student academic records, staff personnel files, financial documents, and administrative records. However, preliminary observation suggested that DIT faced challenges in ensuring the integrity and security of these digital records due to factors such as limited cybersecurity infrastructure, inadequate staff training, and the coexistence of paper-based and digital systems. Without empirical investigation, the extent to which digital record management practices at DIT safeguarded data integrity and security remained unknown, creating a gap that this study sought to address. The rapid digitalization of government services through platforms like Jamii Namba and Jamii X-Change had expanded the collection and processing of personal and organizational data across public and private sectors, yet the mechanisms for protecting this data remained inadequately understood and inconsistently applied. Organizations in Tanzania were confronted with multiple interconnected challenges: limited understanding of how digital record management systems impacted data integrity, leading to potential data corruption, unauthorized modifications, and loss of information authenticity; inadequate knowledge of security threats specific to digital record environments, including insider threats. There existed a critical knowledge gap regarding

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

the specific ways in which digital record management systems could be optimized to enhance both data integrity and security within the Tanzanian context.

1.3 General Objective

To assess the uses of digital record management practices on enhancing data integrity and security.

1.4 Specific Objectives

i. To assess the existing digital record management practices and technologies at Dar es Salaam Institute of Technology (DIT).

ii. To evaluate the technical controls (Example: access control, audit trails, data backup) and policy measures in place to safeguard and protect data integrity and security that DIT used.

iii. To identify the challenges affecting data integrity and security within the current system.

iv. To identify the measures for improving data integrity and security.

1.5 Research Questions

i. What were the prevailing digital record management practices in the selected Dar es Salaam Institute of Technology?

ii. How effective were the existing technical, policy controls in ensuring data integrity and security?

iii. What were the major challenges that compromised data integrity and security?

1.6 Significance of the Study

This study held substantial significance for multiple stakeholders. The research provided actionable insights for improving digital record management systems, reducing risks associated with data integrity failures and security breaches, and enhancing operational efficiency. Organizations could use the findings to optimize resource allocation and develop more effective information governance strategies, where it offered evidence-

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

based recommendations for developing and refining regulatory frameworks that balanced data protection requirements with organizational operational needs, contributing to more effective governance standards, which identified competencies, tools, and strategies essential for managing digital records effectively, supporting professional development and practice improvement in the field. It contributed to the understanding of digital record management, data integrity, and information security, filling gaps in current literature and providing a foundation for future research in this evolving domain. By promoting better data integrity and security practices, it helped protect individual privacy rights, enhance trust in digital systems, and support the reliable functioning of critical societal infrastructure dependent on accurate and secure digital information.

1.7 Scope of the Study

This study focused on digital record management systems, data integrity mechanisms, and security protocols at Dar es Salaam Institute of Technology (DIT). It looked at how DIT managed digital records and how this affected data integrity and security. The study covered: the types of digital records kept at DIT, which included student records, staff records, financial documents, and administrative files. This made it a good place to study digital record management. The systems and technologies used to manage these records were a hybrid record keeping system. It aimed to evaluate how effectively these digital record management systems served as a means for users such as local government officials, researchers, and the general public in data integrity and mechanism in access and retrieval of documents. It encompassed organizations across multiple sectors including healthcare, financial services, government agencies, and educational institutions, allowing for comparative analysis of sector-specific challenges and practices. It provided a legal framework aimed at strengthening data protection and cybersecurity norms among member states, underscoring the growing policy emphasis on securing digital information and safeguarding privacy. Electronic office systems had been introduced to improve transparency, efficiency, and accountability in service delivery. Digital records management inherently intersected with information-security practices, where confidentiality, integrity, and availability were core objectives in protecting data from unauthorized modification, loss, or breaches. It examined the intersection of these

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

three domains, exploring how record management practices influenced both data integrity and security outcomes. Research in information systems emphasized that as data volumes grew, organizational emphasis on security controls and integrity verification had to scale accordingly to prevent vulnerabilities and breaches that could compromise digital assets (Duggineni, 2023).

1.8 Limitations of the Study

The researcher faced the following limitations when conducting this study.

Rapidly Evolving Technology

The digital record management landscape was evolving rapidly, with new technologies, threats, and solutions emerging continuously. Findings might require updates as the technological environment changed. The researcher acknowledged this dynamic nature and focused on foundational principles alongside specific technologies.

Organizational Access and Cooperation: Some organizations were reluctant to share detailed information about their digital record management systems, security measures, and breach incidents due to concerns about competitive disadvantage, reputational risk, or regulatory implications. The researcher addressed this limitation through confidentiality agreements and anonymization of sensitive data. Sensitivity surrounding data security practices limited organizational willingness to share detailed information about vulnerabilities, security incidents, or specific technical implementations, potentially affecting data comprehensiveness. There was a lack of active cooperation from the respondents, who were records managers, because they were occupied with many duties while the study was being carried out.

Generalizability: While the study focused on Tanzania, findings might have limited direct generalizability to other countries with different regulatory frameworks, technological infrastructure, and organizational cultures. However, lessons learned could inform regional initiatives and comparative research. Findings were influenced by the specific organizational contexts, sectors, and geographical regions studied, potentially limiting direct generalizability to all organizational types and global contexts.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Resource Constraints and Financial: Time, budget, and access limitations restricted the sample size, scope of data collection, and depth of analysis possible within the study timeframe. This was a serious problem because the whole process of research needed stationeries and bandwidth, as this study involved online data mostly. But the researcher made some efforts and received assistance from family to accomplish this goal. The study faced limitations in terms of time, budget, and access to specialized technical expertise required for in-depth technical assessments of digital record management systems. The researcher mitigated this through strategic sampling and collaboration with technical experts.

Self-Reporting and Experience: The researcher had little familiarity with conducting research; however, she tried harder to overcome some uncertainty during the study. Where surveys or interviews were used, participants might have overstated their organization's capabilities or underreported security incidents and integrity failures due to reputational concerns or incomplete knowledge.

1.8 Definition of Key Terms

1.8.1 Digital Record Management

The systematic control of digital records throughout their lifecycle (creation, use, maintenance, disposition) to ensure authenticity, reliability, and usability. ISO (2020), ISO 15489-1. Records were documented evidence of activities, decisions, and transactions of an organization, created, received, and maintained as proof of operations. According to ISO 15489 (2016), records were information created, received, and maintained as evidence and information by an organization or person, in pursuit of legal obligations or in the transaction of business. Similarly, Duranti (1997) defined records as reliable and authentic evidence that captured organizational activities and supported accountability.

1.8.2 Data Integrity

The property that data was complete, accurate, consistent, and had not been altered in an unauthorized manner. Often guided by principles like ALCOA (Attributable, Legible, Contemporaneous, Original, Accurate). Katuu, S. (2021).

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

1.8.3 Data Security

The protection of data from unauthorized access, modification, or destruction through measures like encryption, access controls, and network security. Duranti, L. (2022).

1.8.4. Electronic Records Management System (ERMS)

A computerized system used to manage the creation, storage, retrieval, and disposal of digital records in accordance with established policies and standards. Mnjama, N. (2022). Records management referred to the systematic control of records throughout their life cycle, from creation to disposition, to ensure accessibility, reliability, and efficiency. Shepherd and Yeo (2003) defined records management as the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records. Penn, Pennix, and Coulson (1994) described it as the policies and practices that enabled an organization to control its information resources effectively.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter reviewed literature related to digital records management (DRM) and its influence on data integrity and security. The review was organized according to the study objectives: assessment of existing DRM practices and technologies, evaluation of technical and policy controls safeguarding data integrity and security, identification of challenges affecting DRM systems, and examination of measures for improving data integrity and security. The chapter also presented the research gap.

2.0.1 Concept of Digital Records Management

Digital Records Management (DRM) referred to the proper creation, storage, maintenance, use, and disposal of electronic records to ensure they remained authentic, reliable, and usable (ISO, 2020). Good DRM practices included classification systems, metadata management, retention schedules, and access control (Katuu, 2021). Modern systems such as Electronic Document and Records Management Systems (EDRMS), cloud storage, and enterprise content management existed. Unlike traditional paper-based systems, DRM integrated information technologies to manage records throughout their lifecycle. Katuu (2021) explained that effective DRM included classification systems, metadata management, retention scheduling, secure storage, and controlled access mechanisms. Modern DRM technologies incorporated Electronic Document and Records Management Systems (EDRMS), cloud computing platforms, enterprise content management systems, and blockchain-based verification tools (Duranti & Rogers, 2022). In many organizations, DRM supported transparency, accountability, and decision-making.

However, poor implementation could expose records to manipulation and security breaches.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

2.0.2 Concept of Data Integrity

Data integrity meant that information was accurate, complete, and consistent over time. Data integrity referred to the accuracy, completeness, consistency, and reliability of data throughout its lifecycle. It ensured that records remained unaltered except by authorized individuals (Alhassan & Adjei, 2022). According to Duranti and Rogers (2022), data integrity in digital systems depended on proper metadata management, audit trails, system authentication, and access controls. Without such mechanisms, records could lose authenticity and legal validity.

2.0.3 Concept of Data Security

Data security involved protecting digital records from unauthorized access, disclosure, alteration, or destruction. It included technical safeguards such as encryption, firewalls, and access controls, as well as administrative measures like policies and compliance standards (IBM Security, 2024). ISO (2020) emphasized that records management systems needed to include protective controls to maintain confidentiality, integrity, and availability of information.

2.1 Existing Digital Records Management Practices and Technologies

The landscape of digital record management had evolved significantly, transitioning from basic electronic filing systems to sophisticated platforms incorporating artificial intelligence, block chain, and cloud technologies. Shinde, Kirstein, Ghosh, and Franks (2025) conducted a systematic review of 45 papers published between 2011 and 2023, revealing that AI-driven strategies had increasingly been integrated into archival science to streamline recordkeeping processes and improve data retrieval. Their findings highlighted how technologies such as machine learning, natural language processing, and neural networks were being applied to functions including retention scheduling, appraisal, and organization of digital records. Santillán-Lima, Díaz, Piccirilli, Guambo-Vallejo, Duque-Vaca, and Molina-Granja (2025) examined strategic models and international standards for digital preservation through a structured narrative review of 22 studies published between 2010 and 2025. Their analysis identified five critical thematic areas: preservation models, regulatory frameworks, technological tools, institutional

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

diagnostics, and operational challenges. The study documented increasing adoption of standards such as the Open Archival Information System (OAIS) reference model and ISO 16363, alongside integration of emerging technologies including AI, blockchain, and decentralized systems across institutions with varying levels of digital maturity. The practical implementation of digital record management systems varied considerably across sectors. For instance, law enforcement applications demonstrated the specialized nature of modern record management. One commercial solution, the Audax Digital Evidence Management System, illustrated current technological capabilities including role-based access control, redundancy backup mechanisms, cloud or locally hosted storage options, automated data upload, and secure media viewing with audit trail functionality. Similarly, Ricoh's document management approach emphasized three pillars of records management strategy: organization (systematic storage and retrieval), security (controlled access), and compliance (regulatory adherence). However, Pieterse (2025) drew an important distinction between records management systems and preservation systems, arguing they were built on fundamentally different principles. Records management systems prioritized business efficiency high-volume transactions, fast search, workflow integration, and cost-effective storage while preservation systems prioritized permanence, monitoring integrity, managing format obsolescence, and ensuring long-term access and authenticity. This created what Pieterse termed an "architecture gap" that organizations had to navigate when records of enduring value required transition from active management to long-term preservation.

2.2 Evaluation of Technical Controls and Policy Measures for Safe Guarding Data Integrity and Security

Access control mechanisms: Access control represented the first line of defense in protecting digital records. Research demonstrated that role-based access control (RBAC) had emerged as the predominant model for managing permissions in digital record systems. A block chain-based study of digital evidence management in Kenya's National Police Service implemented strict RBAC mechanisms that proved highly effective, achieving a 100% success rate in preventing unauthorized access during security testing. The ISO 27001:2022 standard, particularly Annex a Control 5.33, provided

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

comprehensive guidance on record protection. According to implementation guidance from ISMS. online (2025), effective access control required moving beyond simple password protection to quarterly permission audits, dual approval for sensitive actions, and automated alerts for suspicious access patterns. The standard emphasized that "access is a monitored, time-limited privilege not a set and forget status." Industry best practices further elaborated on access control implementation. Tencent Cloud's technical documentation (2025) advocated for combining RBAC with the principle of least privilege, ensuring backup administrators could manage backups but could not decrypt sensitive data, while compliance teams could audit logs without accessing raw backups. Multi-factor authentication (MFA) and zero-trust architectures were increasingly recommended as essential components of access control frameworks.

Audit trail systems. Audit logging and monitoring constituted critical technical controls for ensuring accountability and traceability. The ISO 27001 framework required that "every access, alteration, and disposal event must be logged, regularly reviewed, and, for high-risk records, require dual authorization." These logs served as the primary evidence for compliance demonstrations and incident investigations. In high-security contexts such as law enforcement, audit trails took on heightened significance. The blockchain model developed for Kenya's National Police Service incorporated an immutable ledger ensuring that all transactions were permanently recorded and verifiable, creating a legally defensible chain of custody for digital evidence. The system achieved 99.9% uptime with average validation times of 2.0 seconds, demonstrating that comprehensive audit logging need not compromise system performance. Cloud-based solutions increasingly integrated automated monitoring capabilities. Tencent Cloud's Cloud Audit service provided detailed logs for operations on backup resources, while automated alerting systems could trigger notifications for anomalous access patterns such as non-admin users downloading large backup files.

Data backup and recovery. Data backup strategies had evolved from simple redundancy to comprehensive approaches incorporating encryption, separation of duties, and regular testing. Technical guidance emphasized encrypting backup data both at rest and in transit using strong algorithms such as AES-256, with encryption keys managed separately from

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

the backup data itself. This separation ensured that even if insiders accessed backup data, it remained unreadable without the corresponding keys. The National Archives and Records Administration (NARA) demonstrated advanced backup and preservation practices through its biennial ISO 16363 self-assessments. As May (2025) documented, NARA evaluated its Electronic Records Archives systems against 115 metrics assessing digital object management, IT infrastructure, security, and organizational policies. This systematic approach ensured that backup and preservation practices maintained alignment with international standards and continuously improved over time. Policy measures and standards. International standards provided the framework within which technical controls operated. The ISO 16363 standard for auditing and certifying trustworthy digital repositories, updated in 2025, required organizations to document policies and procedures across multiple domains. The updated standard introduced new metrics and clarified requirements, emphasizing "documented" rather than merely "written" policies, and expanded terminology to include concepts such as "Preservation Objectives." Similarly, ISO 27001:2022 Annex A Control 5.33 demanded that organizations systematically identify, classify, retain, and securely dispose of all records according to business, legal, and regulatory mandates. The standard moved beyond static policy requirements to demand "traceable, tamper-proof action logs and proven, living compliance."

2.3 Challenges Affecting Data Integrity and Security in Current Systems

Despite technological advances, significant challenges persisted in maintaining data integrity and security within digital record management systems. Santillán-Lima and colleagues (2025) identified persistent gaps in the implementation of sustainable preservation policies, particularly in Latin American contexts, where institutional digital maturity lagged behind technological capabilities.

Operational and Integration Challenges. The integration of emerging technologies introduced its own set of challenges. A qualitative study involving 18 IT specialists and 18 records managers in Nigeria revealed divergent perspectives on blockchain adoption. While IT specialists emphasized blockchain's security features such as decentralization and immutability, records managers expressed concerns about operational challenges

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

including complexity, costs, and integration into existing workflows. Both groups acknowledged blockchain's potential for improving data security but also pointed to scalability and regulatory issues as significant barriers.

Insider Threats and Human Factors. Human factors remained a critical vulnerability. Technical documentation identified insider leakage of backup data as a significant risk requiring multilayered countermeasures. Even with robust technical controls, organizations had to address the human element through employee education, clear policies, and separation of duties.

Records Management and Preservation Divide. The conceptual and technical divide between records management and preservation created challenges for long-term integrity. Pieterse (2025) argued that relying on records management systems for preservation functions "creates a future crisis," as these systems were not designed for permanence. Migration from records management to preservation systems required enhanced metadata, sustainable file formats, remapped relationships, and new access models for unknown future audiences' requirements that many organizations failed to anticipate or resource adequately.

Compliance and Audit Exposure. Common compliance failures documented in the literature included orphaned records (documents losing ownership after staff departures), unmanaged sprawl across multiple platforms, untraceable disposal of sensitive data without formal signoff, and mismatches between written policies and actual practices. These failures created audit blind spots that regulators could exploit, potentially resulting in costly penalties and reputational damage.

2.8 Measures for Improving Data Integrity and Security

Emerging Technological Solution. Block chain technology had emerged as a promising solution for enhancing data integrity through its immutable and decentralized nature. The Kenyan law enforcement study demonstrated blockchain's transformative potential, achieving 100% data immutability and 98% transaction success rates. The model integrated key security features including an immutable ledger, role-based access control, SQL injection resistance, and seamless interoperability with existing systems. However,

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

as the Nigerian study revealed, realizing these benefits required addressing operational challenges and building consensus between technical and operational stakeholders.

Artificial intelligence applications. AI technologies were increasingly deployed to enhance data integrity and security. Shinde and colleagues (2025) documented AI applications including content-based exploration of archival images using neural networks, named entity recognition in historical documents, and machine learning for predicting high-risk cases. These applications promised to streamline recordkeeping processes while improving the accuracy and reliability of data management. However, the authors emphasized the necessity for enhanced interdisciplinary collaboration between AI experts and archival professionals to ensure these technologies met actual needs and maintained appropriate ethical standards.

Standards-based approaches. Adherence to international standards represented a fundamental measure for ensuring data integrity and security. The OAIS reference model (ISO 14721) and ISO 16363 provided structured frameworks for developing and evaluating trustworthy digital repositories. NARA's biennial self-assessments demonstrated how systematic application of these standards enabled organizations to document successes, identify improvement areas, and maintain accountability to global benchmarks.

ISO 27001's comprehensive approach to record protection encompassed the entire record lifecycle from creation and retention to secure destruction. The standard required demonstrable evidence that records were under control regardless of storage location, with clear ownership, monitored access, and auditable processes.

Integrated control frameworks. Effective measures combined multiple control types into coherent frameworks. Technical guidance advocated for layered approaches incorporating access control, encryption, audit logging, separation of duties, and data masking. When implemented together, these measures created defense-in-depth that addressed diverse threat vectors. Similarly, records management strategy had to integrate organization, security, and compliance considerations while standardizing workflows, creating information hierarchies, enforcing permissions, and conducting regular audits.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

2.9 Conceptual Framework

The conceptual framework showed the relationship between digital records management practices, technical controls, and policy measures (independent variables) and data integrity and data security (dependent variables). Independent Variables (what affected the outcome): Digital record management practices (how records were created, stored, and used), Technical controls (access control, audit trails, backup), Policy measures (rules, guidelines, standards). Dependent Variables (the outcomes being studied): Data integrity (accuracy, completeness, consistency), Data security (protection from unauthorized access, loss, or damage).

The framework also showed that there were challenges (like insider threats, technology gaps, and limited resources) that made it harder to achieve good outcomes.

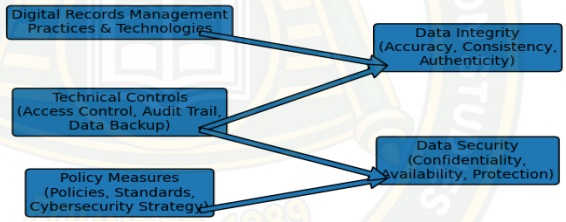


Figure 1

Conceptual Framework Showing the Relationship Between Digital Records Management and Data Integrity and Security. Source: Researcher (2026)

2.10 Research Gap

Although many studies discussed digital records management and cybersecurity globally, limited research integrated DRM practices, technical controls, and policy measures together in Tanzania.

There was also limited empirical evidence linking DRM directly to data integrity and security outcomes. This study aimed to fill this gap. Insufficient attention had been paid

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

to the Records Management Preservation Continuum. Pieterse (2025) articulated a fundamental distinction between records management and preservation systems, yet the literature largely treated these as separate domains rather than as interconnected stages in a continuum. This separation created knowledge gaps regarding how organizations should manage transitions from active records management to long-term preservation. Questions remained about optimal timing for migration, metadata requirements for preservation readiness, and sustainable resourcing models for preservation functions. The proposed study examined how current systems addressed or neglected these transition requirements, potentially identifying best practices and common failure points.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter explained various aspects that were applied in carrying out the research study. It explained the research design, research approach, target population, area of the study, sample size, sampling technique, validity and reliability, and ethical considerations were also included.

3.1 Research Design

According to Bell, Bryman, & Harley (2019), research design was a framework for the collection and analysis of data. The most important decision in research design was the choice to be made concerning the research approach since it helped to determine how a particular study would be. The researcher employed a Case Study design. In this study, the researcher decided to use a Single Case Study Design.

3.1.1 Single Case Design

This was a kind of Case Study Design where the study investigated a single case to get in-depth information (Matthew and Liz, 2015). This design enabled a researcher to study a single institution to get detailed information in such a case (institution). The researcher used this design because she wanted to study a single institution (only one academic institution).

3.2 Research Approach

A research approach was a plan of action that gave direction to conduct research systematically and efficiently (Daniel, 2016). The research methodology comprised three research approaches according to Neuman (2003), which were qualitative, quantitative, and mixed. The researcher used a mixed approach where both qualitative and quantitative methods were used to collect and analyze data. In this study, these approaches helped the researcher to obtain more details and specific information about the problem of the study. It also gave freedom to the researcher to use narration and numbers during data analysis. Creswell and Plano (2006) supported the researcher's use of a mixed approach, as it

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

allowed the collection of a wider range of data for a deeper and clearer understanding of the problem.

3.2.1 Mixed Approach

Creswell (2014) defined a mixed approach as one in which data collection and analysis were carried out using both qualitative and quantitative methods in a single study. Mixed research approach meant the amalgamation of both qualitative and quantitative methods in the same study. The use of quantitative and qualitative approaches in combination provided a better understanding of research problems and complex phenomena than either approach alone (Creswell and Clark, 2017).

3.3 Area of the Study

Ngechu (2006) defined an area of study as the limit of the study or problem. The study was conducted at Dar es Salaam Institute of Technology (DIT). DIT was a higher learning institution located in Dar es Salaam, Tanzania. It was established to provide education and research in engineering, science, and technology. DIT had several campuses, with the main campus in the city of Dar es Salaam.

DIT was chosen because of the digital transformation in DIT, which had been adopting digital systems for managing records. This included student records, staff records, financial documents, and administrative files. This made it a good place to study digital record management. DIT handled many different types of records; some were very sensitive, like student grades and personal staff information. These needed to be kept accurate and secure. The researcher was familiar with DIT and could easily reach the people who needed to be involved in the study. This made data collection easier and faster. Not many studies had looked at digital record management in Tanzanian higher education institutions; studying DIT helped fill this gap. DIT managed records for thousands of students and staff, and the institution had a registry that produced and a department that handled official records. There was also an ICT department that managed computer systems. DIT used both paper and digital systems, which was common in Tanzania.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

3.4 Population

According to Cresswell (2012), a population was defined as a group of individuals who had similar features that helped them to be different from other groups, as it could be an entire collection of people, animals, plants, or things from which data may be collected. It was the entire group the researcher was interested in and wished to describe or draw a conclusion about (Kombo & Tromp, 2006). In this study, the researcher used a population of 50 respondents from Dar Es Salaam Institute of Technology.

3.5 Sample Size

A sample was one that could be taken as representative of the whole population, whereby its results could be generalized (Kothari, 2004). Also, sample size was the number of sampling units included in a sample (Saman, 2003). A total of fifty (50) respondents were selected to participate in this study, whereby twenty-five (25) respondents were responsible for filling in the questionnaire and were staff from the Registry at Dar Es Salaam Institute of Technology, and the other twenty-five (25) respondents were stakeholders like government officers, researchers, and the general public.

The sample size of this study was obtained by using the formula introduced by Taro Yamane (1964) as cited by Johnson (2011), which stated that:

$n = N / (1 + N(e)^2)$

Whereby: n = sample size; N = number of population = 50; e = number of acceptable error = 0.1

$n = 50 / (1 + 50(0.01)^2)$; $n = 50 / (1 + 1.5)$

If n = 25.

3.6 Sampling Procedures

Sampling techniques were methods researchers used to select a population's representatives that could be used to make inferences or generalizations about the whole population concerning an existing theory (Taherdoost, 2018). In this study, both probability and non-probability sampling techniques were used to select the sample

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

required by the study. The probability sampling technique used in the study was the random sampling technique. This technique was used to select record assistants to fill in questionnaires. On the other hand, a non-probability technique called purposive or judgmental sampling was used to obtain the key informant, a record officer who was included in interviews.

3.6.1 Simple Random Sampling Technique

Simple random sampling referred to the kind of probability sampling which required that each member of the population have an equal chance of being selected or included as a sample (Verma, et al., 2017). In this study, simple random sampling was used so as to eliminate bias by giving all people in a field area an equal chance to be selected in the study.

3.6.2 Purposive Sampling Techniques

According to Glenton & Lewin (2019), purposive sampling was a method that belonged to the category of non-probability sampling techniques that permitted a researcher to select samples on the basis of their knowledge, relationships, and expertise in relation to the objective of the study. In this study, this method was used to get key information which could not be attained from other techniques, where twenty-five (25) respondents (archive officers) from a sample size of fifty (50) were key informants.

3.7 Data Collection Method

Data collection was the systematic process of gathering and measuring information on the variable of interest in an established style that enabled one to answer stated research questions (Kabir, 2016). In this study, the researcher used two major sources of data collection which included primary and secondary sources, since the combination of these methods improved validity and reliability.

3.7.1 Primary Data

Primary data referred to data from sources that the researcher directly collected through interviews, observation, and questionnaires (Glenton & Lewin, 2019). Primary data were

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

those which were collected fresh for the first time, and thus were original. Primary data were collected from the sample population by using the questionnaire method.

3.7.1.1 Questionnaire Method

According to Kabir (2016), a questionnaire was a research tool which included a series of written and printed questions that were in a systematic order to gather information from the respondents, then allowing them to attempt the questions individually and yield the filled queries to the researcher. In this study, the researcher applied both close-ended and open-ended questions, whereas open-ended questions provided freedom to respondents to provide more details, while close-ended questions usually did not provide freedom to the respondents for more explanation (Creswell, 2012). This study applied the questionnaire method to Dar Es Salaam City Council staff, since it helped to eliminate bias among the respondents.

3.7.1.2 Interview Method

Interview was one of the instruments of data collection that involved a one-to-one meeting at which one was asked the target questions related to the research problem (Rwagoshora, 2006). This study used a semi-structured interview to obtain data, whereas a semi-structured interview was a kind of interview that employed a blend of closed-ended questions and open-ended questions. The researcher used this method to collect key information from the record officer since it allowed rearranging any query accordingly to acquire appropriate information.

3.7.2 Secondary Data

Secondary data referred to data that was collected by someone other than the user (Raj, 2005). Secondary data were collected by reviewing documents related to the study. Secondary data in this study were collected through reviewing research reports of other scholars' theses and dissertations, books, journals, and articles (secondary sources) related to the study.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

3.8 Data Analysis and Processing

Krishna (2019) defined data analysis as the means of critical examination of the assembled and grouped data for studying the characteristics of the object under study and for defining arrangements of association among the variables connected to it. The researcher obtained both quantitative and qualitative data, and each had its own way of being analyzed. As with quantitative data, it could be analyzed by a statistical method using Excel and the Statistical Product and Service Solutions (SPSS), but qualitative data were analyzed using the content analysis method, since qualitative data were in the form of words, not numerical data.

3.9 Pilot Study

This was referred to as a pre-study, which was defined as a small study, a pilot study carried out to ensure the validity and reliability of the research instruments. A pilot study was typically conducted with a small representative sample identical to but not including the group to be studied Orodho (2010) further stated that the main reason for conducting the pilot study was to test the weaknesses and strengths of research instruments to correct their weaknesses and also help the researcher become familiar with the research instruments.

3.9 Validity and Reliability

Creswell (2012) was of the view that validity was the development of sound evidence to demonstrate that the test interpretation matched its proposed use. That meant validity was about testing the instruments to see whether they measured what was intended to be measured, thus bringing the intended results. While reliability was about the degree to which a particular measuring procedure gave similar results over several repeated trials, he further added that if the results were different, then the measurement was not reliable.

3.9.1 Validity. Validity was defined as the accuracy of measurement. It valued the efficiency of tools and instruments applied in the study (Creswell & Creswell, 2018). For instance, the study's questionnaires were effectively framed and tested prior to the research with the objectivity for which the research objectives were meant. Construct validity was ensured through the review of various literature related to the study.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

3.9.2 Reliability.

Reliability was the constancy of a research measurement and the degree to which the study's instruments examined and provided similar feedback each time they were used in a similar environment with similar subjects (Gerring, 2023). The study was reliable when it consistently measured what it was expected to examine; this was when similar results were repeated.

3.10 Research Ethics

Research ethics required a researcher to follow appropriate guidelines and rules for protecting participants' dignity as well as publishing relevant and ethically oriented information (Kothari, 2019). This also referred to things which should or should not be done by the researcher before, during, and after obtaining the data from the field (Bhattacherjee, 2021).

To ensure ethical consideration, the researcher introduced the purpose of the research to the respondents; this brought honesty and cooperation to participate in the study. Also, the researcher used the information obtained from the field for academic purposes only while maintaining the confidentiality of the respondents who participated in this study. Lastly, the researcher ensured that all relevant sources involved in this study were acknowledged to avoid plagiarism in conducting this research.

3.11 Chapter Summary

This chapter discussed the research methodology and methods used in the study to address the research problem. This included a comprehensive discussion of the research design, research approach, data collection methods, and other issues such as study population and ethical considerations.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION

4.0 Introduction

This chapter presents the findings of the study. The study looked at how digital record management is used to protect data integrity and security at the Dar es Salaam Institute of Technology (DIT). Data were collected from 50 participants. Twenty-five (25) of them were Registry staff, and twenty-five (25) were other stakeholders, such as government officers, researchers, and members of the public who use DIT records. The data collected from respondents through questionnaires, interviews, and observations are analyzed and interpreted in relation to the study objectives. The chapter includes data presentation using tables and figures, followed by an analysis and interpretation of the results. Key themes explored include the availability of the general structure of the workforce in ICT and records management departments, accessibility challenges, user satisfaction, and the effectiveness of digital record management systems. The findings provide insights into the extent to which users utilize digital records and the barriers they encounter in the process.

It is also worth noting, as a methodological caveat, that percentages reported for questions permitting multiple responses (for example, the challenges and improvement-measures items) do not sum to 100 percent, since a single respondent could select more than one option. Where this applies it is indicated explicitly in the surrounding text so that the figures are not misread as mutually exclusive categories.

4.1 Demographic Information of Participants

This section describes the background of the participants who took part in the study. Knowing their gender, education, and age helps us understanding the sample better.

4.1.1 Gender of Participants

The respondents were asked to indicate their gender; Information on gender of respondents was needed by researcher so as to identify their participation of respondents depending to

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

their gender. The study shows that both male and female were used to escape bias where Table summarizes the results Participants were asked about their gender. Figure 4.1 shows the results.

Table 4.1: Gender of Participants (n=50)

Gender of Participants	Frequent	Percentage (%)
Male	30	60%
Female	20	40%
Total	50	100%

Source: Field Study (2026)

The results show that men were the majority, representing 60 percent (30 people) of all participants, while women represented 40 percent (20 people). This reflects the general structure of the workforce in ICT and records management departments in Tanzania, where men still predominate. The imbalance is consistent with broader patterns reported across sub-Saharan African public-sector ICT functions, where women remain under-represented in technical roles despite comprising a growing share of clerical and administrative records staff. This has a practical implication for training design: if digital-skills interventions at DIT are to close rather than widen this gap, they may need to include deliberate outreach and scheduling accommodations that make participation easier for women staff, who may carry disproportionate domestic responsibilities alongside their institutional duties.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Figure 4.1: Gender of Participants (n=50)

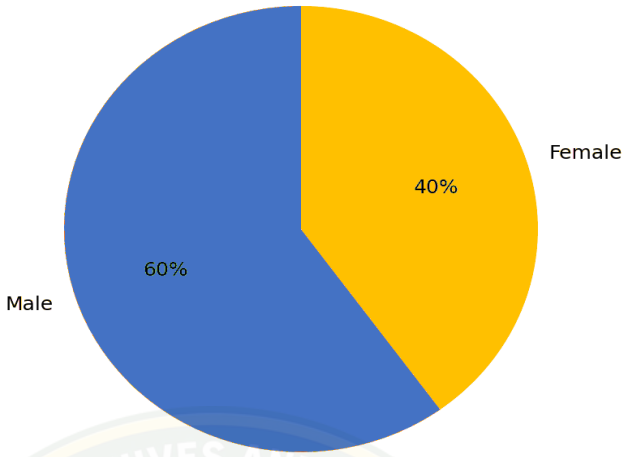


Figure 4.1: Gender of Participants (n=50)

Source: Field Study (2026)

4.1.2 Education Level of Participants

Educational level was important for understanding participants' capacity to use and understand digital records management systems were also asked about their highest level of education. Depending to their level of education and data are indicated in table 4.2 below.

Table 4.2: Education Level of Participants (n=50)

Gender of Participants	Frequent	Percentage (%)
Certificate	8	16%
Diploma	12	24%
Degree	20	40%
Master's Degree	10	20%
total	50	100%

Source: Field Study (2026)

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

As shown in Figure 4.2, most participants held a Bachelor's Degree, representing 20 participants (40%), followed by Diploma holders at 12 (24%), Master's degree holders at 10 (20%), and Certificate holders at 8 (16%). These results indicate that DIT has sufficiently educated staff to handle digital systems. Taken together, 60 percent of the sample held a Bachelor's degree or higher, suggesting that the constraint on digital records management performance at DIT is less likely to be a shortage of formal education and more likely to be a shortage of specific, applied training on records-management tools, standards, and security practice a distinction that becomes important later in the chapter when staff training emerges as the challenge cited most frequently by respondents.

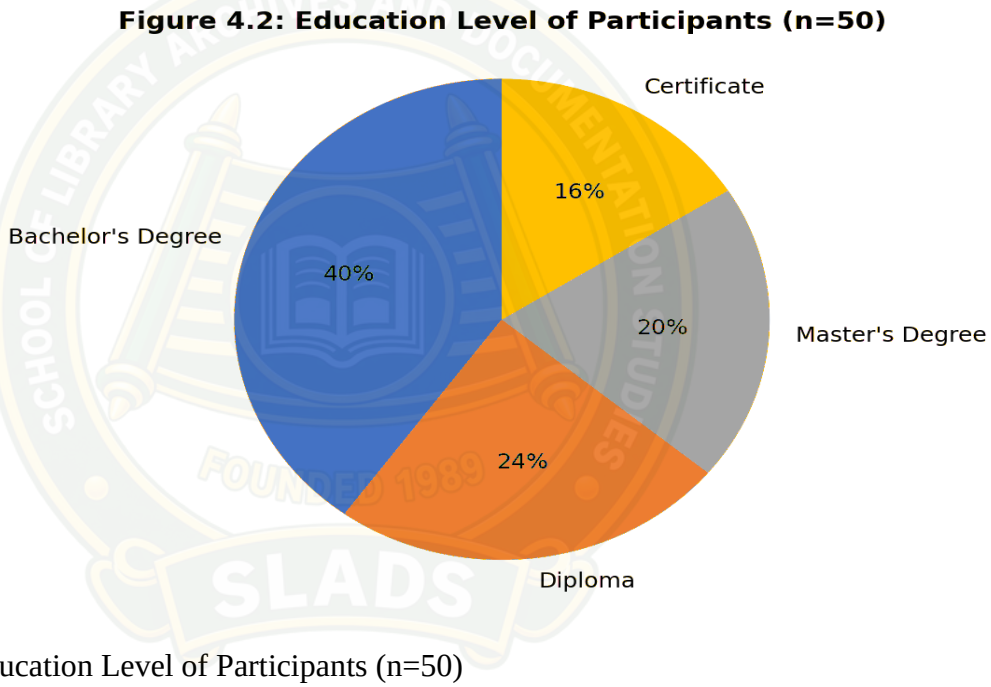


Figure 4.2: Education Level of Participants (n=50)

Source: Field Study (2026)

The findings imply that the majority of the respondents have attained a higher level of education, with a significant proportion holding degrees. The data on the educational levels of participants in the DIT provides a clear picture of the sample's composition, heavily weighted towards certificate and diploma students. This demographic characteristic is fundamental to interpreting the study's results on how digital record management is used to strengthen data integrity and security, as it suggests that the findings primarily reflect the

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

experiences and behaviors of record management. Understanding this distribution is essential for accurately assessing the scope and applicability of the research outcomes.

4.1.3 Age Group of Participants

Participants were asked which age group they belong. The respondents were requested to mention their respective age. The question was asked to the respondents in this study due to its different ages where table 4.3 below summarized the results

Age Groups of Participants	Frequent	Percentage (%)
20-28	10	20%
29-34	14	28%
35-44	16	32%
45 and above age	10	20%
total	50	100%

Table 4.3: Age Groups of Participants (n=50)

Source: Field Study (2026)

Figure 4.3 shows that the largest group of participants was aged 35-44 (16 people, 32%), followed by the 29-34 age group (14 people, 28%), the 20-28 age group (10 people, 20%), and the 45-and-above age group (10 people, 20%). This shows that most DIT staff are of working age and have sufficient experience to handle modern systems. Combining the two youngest brackets (20-34 years) accounts for 48 percent of the sample, a cohort typically associated in the literature with greater comfort adopting new digital tools; this age structure is therefore an asset that DIT can leverage when introducing more advanced systems, provided that training programmers are designed inclusively enough to also bring the older, more experienced 45-and-above cohort along, since this group often holds the greatest

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

institutional memory regarding legacy paper records

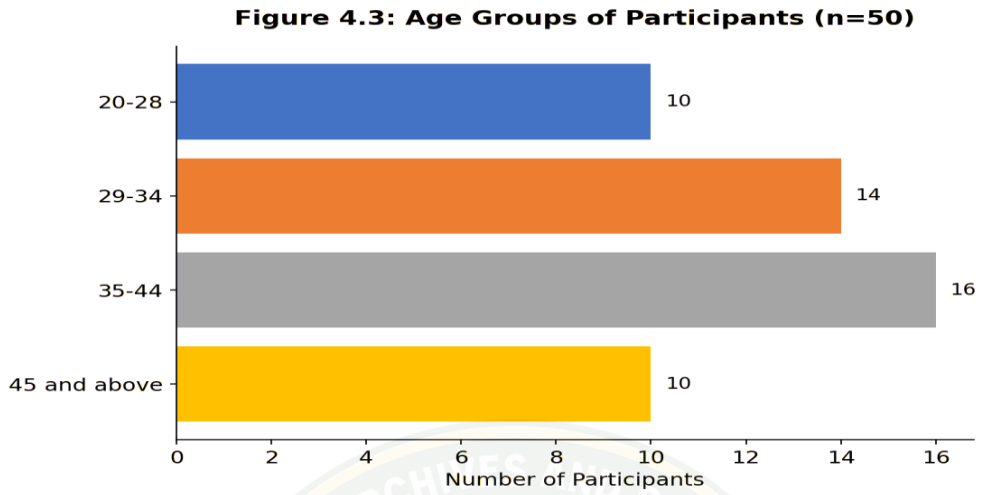


Figure 4.3: Age Groups of Participants (n=50)

Source: Field Study (2026)

4.2 Existing Digital Record Management Practices and Technologies at Dit

The first objective of the study was to find out the digital record management practices and technologies that are already being used at DIT.

4.2.1 How Participants Access Digital Records

This section assesses how to find the records they need and it provides insights into the effectiveness of the digital record management system's organization and search ability Participants were asked how they usually access records at DIT.

Participants were asked how they access digital records. Most (46 percent) said they use both methods online access and physical visits. This shows that the hybrid system still dominates at DIT. Thirty percent used online access only, while 24 percent relied on physical visits only.

The fact that fewer than a third of respondents can rely on online access alone points to gaps in remote-access infrastructure, single sign-on provisioning, or network reliability, any of which would force users back onto a physical-visit workflow. This has knock-on implications for data integrity, since every physical retrieval of a record represents a point at which the record can be mishandled, misfiled, or altered without a corresponding digital audit entry.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Table 4.4: Show Participants Access Digital Records

(n=50)

Participants Access Digital Records	Frequent	Percentage (%)
Physical visit	8	24%
Online access	12	30%
Physical and online access	30	46%
Total	50	100%

Source: Field Study (2026)

The results show that 50 percent of participants expressed some degree of satisfaction (Very Satisfied 20% and Satisfied 30%), while 26 percent were neutral. Those who were dissatisfied (Dissatisfied and Very Dissatisfied) accounted for 24 percent. These results indicate that although the system has achieved some success, there is still considerable room to improve its effectiveness.

Read alongside the systems-in-use data above, this satisfaction profile suggests that user experience is being shaped less by the choice of technology platform per se and more by inconsistent access and reliability: a neutral-to-dissatisfied combined proportion of 50 percent is a meaningful signal that the system, in its current hybrid form, is not yet dependable enough to be trusted by half of its user base for routine information retrieval.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

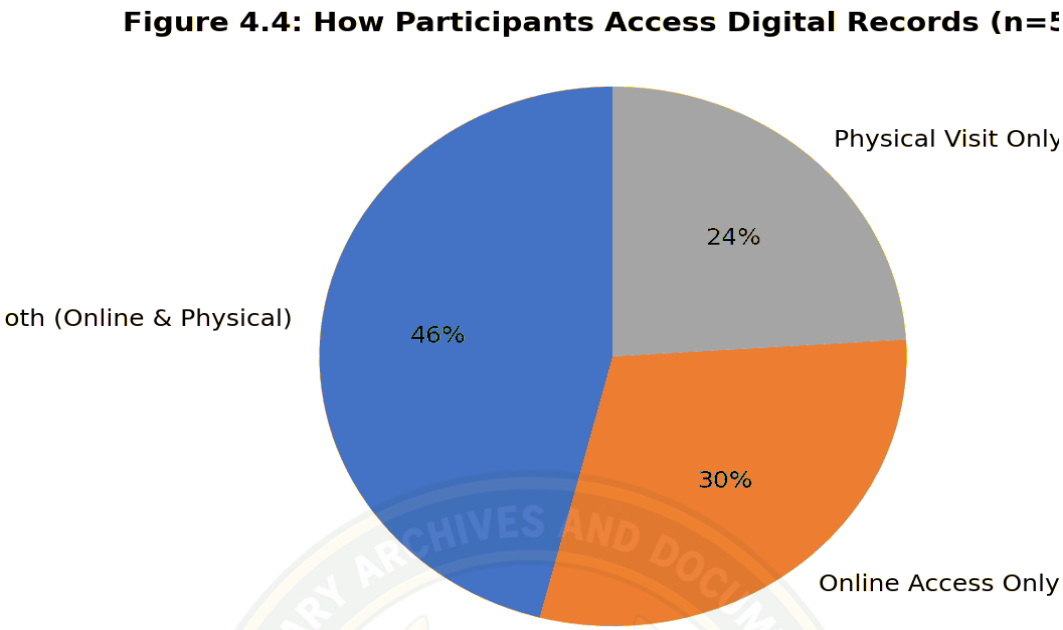


Figure 4.4: How Participants Access Digital Records (n=50)

Source: Field Study (2026)

4.2.2 Ease of Locating Record Materials

Participants were asked how easy it is to find the records they need this section assesses how easy or difficult it is for users to locate the materials they need within the registry. It provides insights into the effectiveness of the digital record management system's organization and search ability.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Table 4.5: Ease of Locating Record Materials

(n=50)

Ease of Locating Record Materials	Frequent	Percentage (%)
Very easy	8	16%
Easy	14	28%
Neutral	13	26%
Difficult	11	22%
Very difficult	4	8%
Total	50	100%

Source: Field Study (2026)

The results were mixed. Sixteen percent found it very easy, and 28 percent found it easy, making a total of 44 percent who did not struggle to find records. However, 26 percent were neutral, 22 percent found it difficult, and 8 percent found it very difficult. This means more than half of the participants still face some level of difficulty when trying to locate records. This may be linked to poor indexing and the continued use of paper files alongside digital ones.

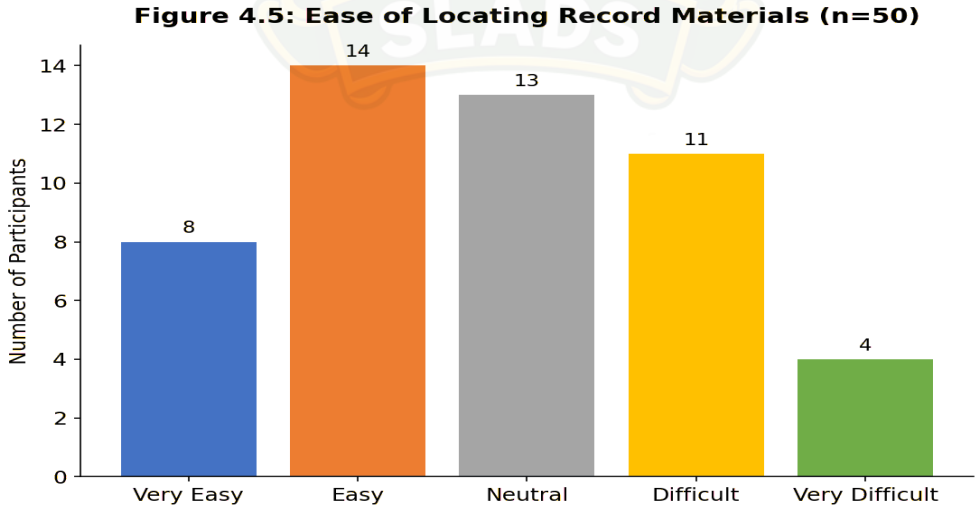


Figure 4.5: Ease of Locating Record Materials (n=50)

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Source: Field Study (2026)

4.2.3 Relevance of Information Retrieved

This section examines how relevant the information retrieved from the digital Record System is to users' needs. The findings reveal the extent to which the archival materials meet user expectations for relevance and usefulness. Participants were asked whether the information they get from the digital record system is relevant to their needs.

Table 4.6: Relevance of Information Retrieved from the Digital Record System (n=50)

Relevance of Information Retrieved	Frequent	Percentage (%)
highly relevant	34	58%
Neutral	9	24%
highly irrelevant	7	18%
Total	50	100%

Source: Field Study (2026)

The results show that 58 percent of participants found the information either highly relevant or relevant. Twenty-four percent were neutral, while 18 percent said the information was irrelevant or highly irrelevant. This shows that although the system is useful for most users, it still does not fully meet the needs of a good number of participants.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

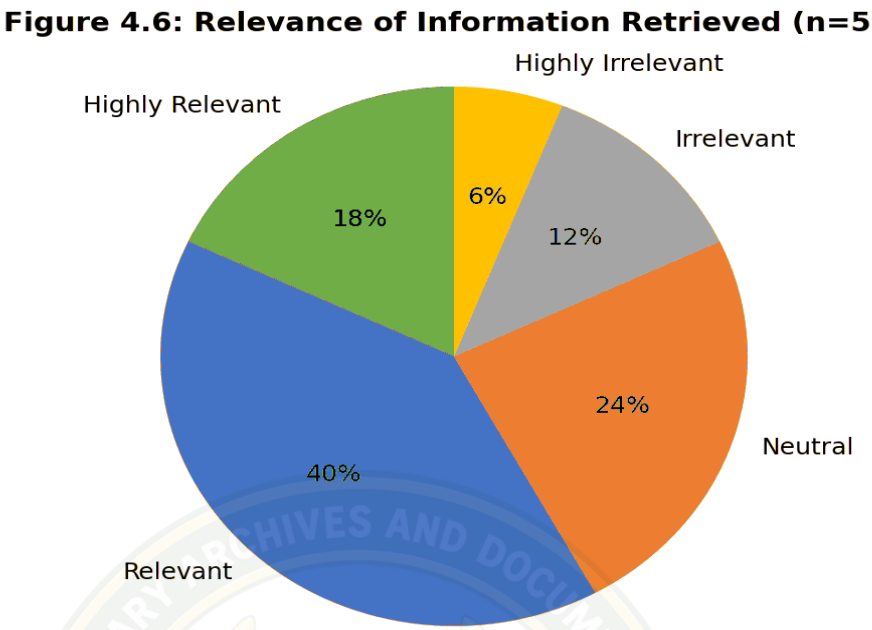


Figure 4.6: Relevance of Information Retrieved from the Digital Record System (n=50)

Source: Field Study (2026)

4.2.4 Interview Findings on Current Practices

Interviews with records officers gave more details about how the system works day to day.

We use a hybrid system. Older records are kept on paper, while newer ones are stored on the computer. This makes it easier for some tasks but harder for others, because we have to check two places sometimes.

Users sometimes ask for documents that are not yet in the digital system. When this happens, we have to search through the paper files, which takes more time.

These interview answers support the questionnaire findings. They show that DIT is still in the middle of moving from paper to fully digital records. This transition stage, known as a hybrid system, is common in many public institutions in Tanzania (Mnjama & Wamukoya, 2022).

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

4.3 Technical Controls and Policies for Protecting Data Integrity and Security

The second objective of the study was to check the technical controls, such as access control, audit trails, and data backup, and the policies that DIT uses to protect data integrity and security.

4.3.1 Effectiveness of Technical Controls

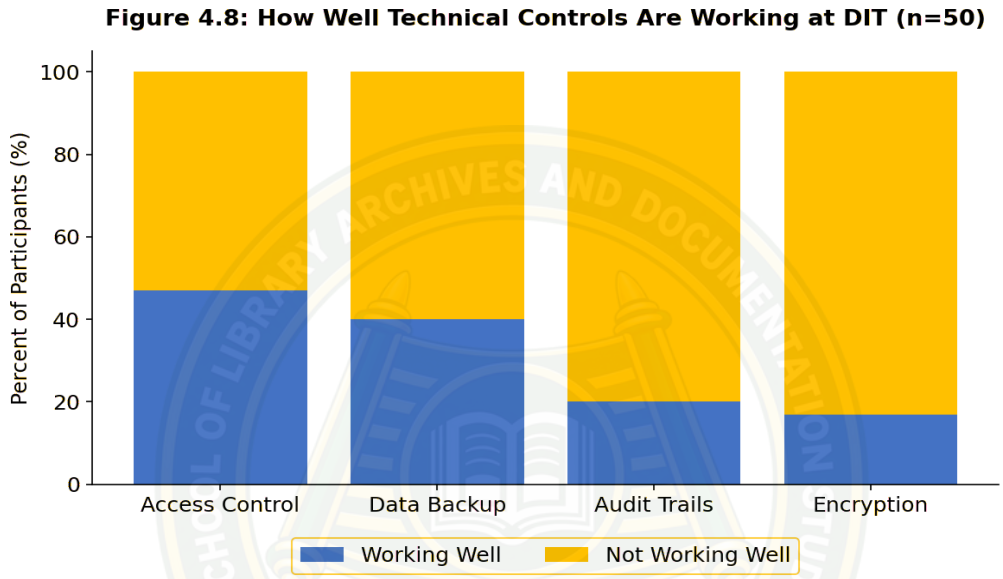


Figure 4.7: how well technical controls are working at DIT (n=50)

Source: Field Study (2026)

Figure 4.7 shows that access control was the most effective, with 14 participants (47%) rating it as adequate, while data backup was rated as adequate by 12 participants (40%). However, audit trails and encryption were seen as the weakest in implementation, with more than 15 and 17 participants respectively saying they were not functioning well.

This is consistent with the findings of Duranti and Rogers (2022), who noted that without robust metadata controls, audit trails, and system authentication, records can lose their authenticity and legal force. It is also similar to the study by Alhassan and Adjei (2022), which found that data integrity requires strong control systems, which remain a challenge for many African institutions.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

It is notable that the two weakest controls audit trails and encryption are precisely the mechanisms that allow an institution to detect and prove tampering after the fact, as opposed to access control and backup, which primarily prevent loss or unauthorized entry going forward. Their weak implementation means that even where access control succeeds in keeping unauthorized users out, DIT currently has limited ability to demonstrate, to an auditor, a court, or a data-protection regulator, exactly who accessed or altered a given record and when. This is precisely the gap that the Personal Data Protection Act (PDPA 2023) and ISO 27001:2022 are designed to close, and it represents one of the more urgent technical priorities emerging from the study.

4.3.2 Interview Findings: Views of Records Officers

Interviews with records officers conducted at DIT revealed further important information about technical controls. Officers were asked several questions, including how digital systems are organized and how records efficiency is measured.

We use a Hybrid system where older records are kept on paper and recent ones are stored on computer. But the problem is that even the computerized records are not secure enough, because many staff members can access files without restriction.

Our backup system is not scheduled regularly. Often, we only back up when the system breaks down, which is not a good way of protecting our important data.

This information shows that DIT still has major weaknesses in technical controls, particularly in the areas of access management, audit trails, and routine backups areas that ISO 27001:2022 identifies as pillars of data security.

The officers' own words add a layer of nuance the quantitative data cannot capture on its own: the phrase 'we only back up when the system breaks down' describes a reactive rather than scheduled backup culture, meaning that the institution's recovery point in the event of a serious incident could, in the worst case, be measured in weeks or months of unprotected activity rather than hours. Likewise, unrestricted internal access flagged independently by more than one officer is a classic precursor to insider-threat incidents, a concern that recurs again in Section 4.4.3 below

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

4.3.3 Satisfaction with the Digital Record System

This section explores the level of satisfaction among respondents regarding the system's ability to meet their information needs. It includes an assessment of how well the system provides users with the information they require and the overall experience of accessing these materials. Participants were also asked how satisfied they are with the ability of the digital record system to give them the information they need.

Figure 4.7: Satisfaction with the Digital Record System (n=50)

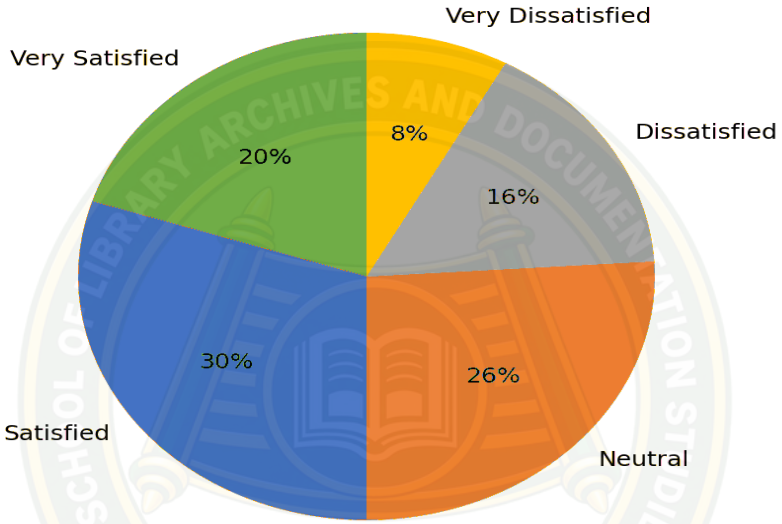


Figure 4.8: Satisfaction with the Digital Record System (n=50)

Source: Field Study (2026)

The results show that 50 percent of participants expressed some degree of satisfaction (Very Satisfied 20% and Satisfied 30%), while 26 percent were neutral. Those who were dissatisfied (Dissatisfied and Very Dissatisfied) accounted for 24 percent. These results indicate that although the system has achieved some success, there is still considerable room to improve its effectiveness.

Read alongside the systems-in-use data above, this satisfaction profile suggests that user experience is being shaped less by the choice of technology platform per se and more by inconsistent access and reliability: a neutral-to-dissatisfied combined proportion of 50 percent

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

is a meaningful signal that the system, in its current hybrid form, is not yet dependable enough to be trusted by half of its user base for routine information retrieval.

4.3.4 Interview Findings on Technical Controls

We do not have a clear schedule for backing up our data. Most times we only back up when the system has a problem, which is risky.

Many staff can access files without any restriction. This is not safe, because anyone can open or change a record even if it is not their work.

These comments show that DIT still has weaknesses in how it manages access to records and how often it backs up data. Both are important pillars of data security according to ISO 27001:2022.

4.4 Challenges Affecting Data Integrity and Security in the Current System

The third objective of the study was to find out the challenges that affect data integrity and security in the current system at DIT.

4.4.1 Main Challenges Identified

Figure 4.9: Challenges Affecting Data Integrity and Security (n=5

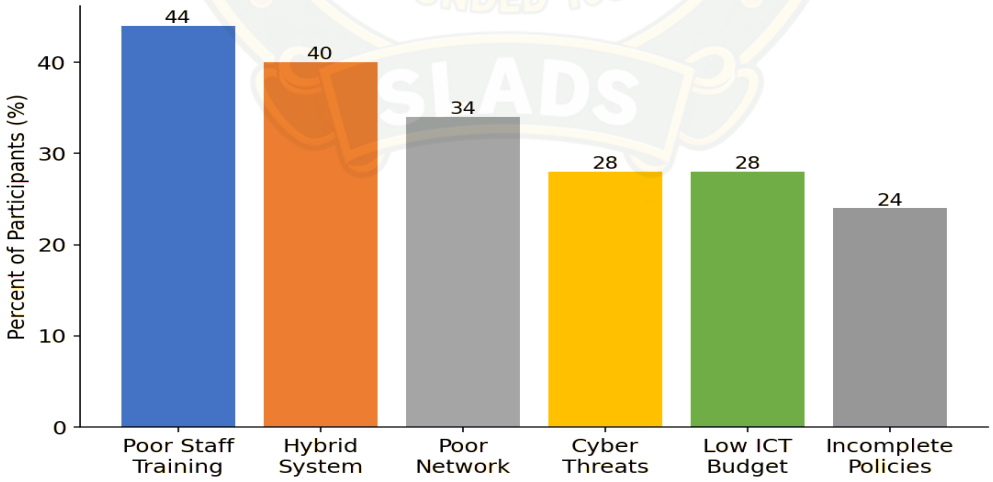


Figure 4.9: Challenges Affecting Data Integrity and Security (n=50)

Source: Field Study (2026)

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Poor staff training was the biggest challenge, mentioned by 44 percent of participants. This was followed by the hybrid system at 40 percent, poor network connection at 34 percent, cyber threats at 28 percent, low ICT budget at 28 percent, and incomplete policies at 24 percent. Participants were allowed to choose more than one challenge, so the numbers add up to more than 100 percent.

These findings are similar to those of Ngoepe and Saurombe (2022), who found that African institutions often face the same set of challenges: not enough training, weak infrastructure, and low budgets for ICT.

4.4.2 Challenges Faced When Accessing Digital Records

This section identifies the common challenges faced by users when attempting to access digital records materials. The findings address issues such as outdated systems, lack of proper indexing, limited accessibility, and insufficient staff support. Participants were also asked about the specific problems they face when trying to access digital records.

Indexing emerges here as the single largest accessibility complaint, which is consistent with the earlier finding that EDRMS adoption the category of system that typically provides structured metadata and search remains low. Improving indexing is therefore likely to be a comparatively low-cost, high-impact intervention relative to a full platform replacement, since it can often be addressed by retrofitting metadata standards onto existing digital holdings rather than procuring entirely new infrastructure.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

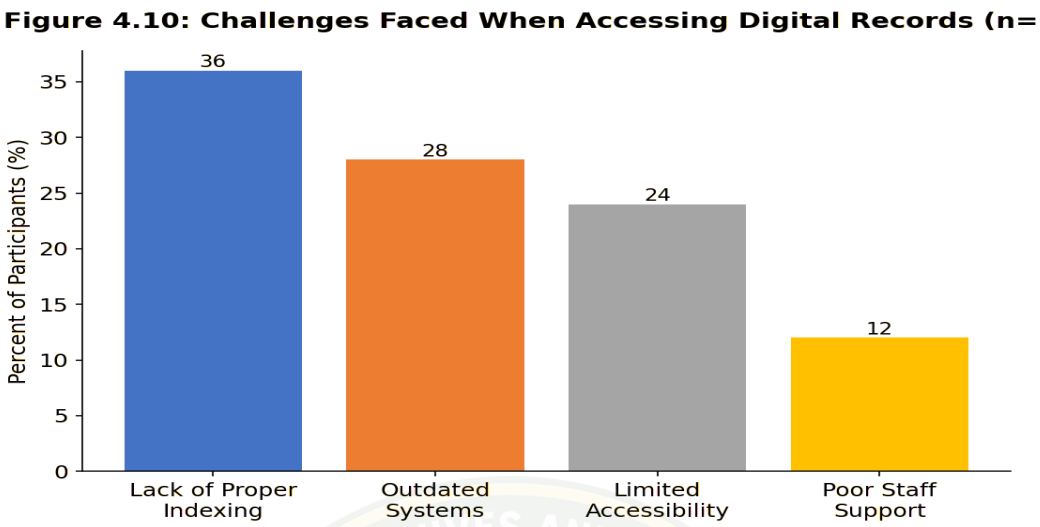


Figure 4.10: Challenges Faced When Accessing Digital Records (n=50)

Source: Field Study (2026)

The biggest problem was lack of proper indexing, mentioned by 36 percent of participants. This means records are not well organized, making them hard to find. This was followed by outdated systems at 28 percent, limited accessibility at 24 percent, and poor staff support at 12 percent.

4.4.3 Interview Findings on Challenges

Cyber threats are increasing. We do not yet have a strong system to protect us from viruses or hacking.

Some staff can view records they should not be able to see. This puts our data at risk from the inside, not just from outside attackers.

This matches the Interpol (2023) report, which found that cybercrime is increasing in public institutions across Africa. It also matches the findings of Mwanga and Kessy (2022), who reported similar cybersecurity challenges in Tanzanian public institutions.

Cyber threats were identified as another rapidly growing challenge. Records officers explained that DIT does not yet have a comprehensive system to protect itself against cyber-attacks such as viruses, hacking, and internal data leaks (insider threats). This is consistent with an Interpol (2023) report that showed an increase in cybercrime in public institutions

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

across Africa, and with Mwanga and Kessy (2022), who reported cybersecurity challenges in public institutions in Tanzania.

The explicit mention of insider threats alongside external hacking is significant: it echoes the unrestricted-access concern raised independently in the interviews (Section 4.3.2), suggesting that the institution's most immediate cybersecurity exposure may not be a sophisticated external attacker but rather the everyday, low-friction ability of authorized staff to view or copy records beyond what their role requires. Addressing this typically costs far less than defending against advanced external threats, since it depends primarily on role-based access configuration rather than new hardware or software investment.

4.5 Measures to Improve Data Integrity and Security

The fourth objective of the study was to find out what measures are needed to improve data integrity and security in the digital record management system at DIT.

4.5.1 Participants' Recommendations

Figure 4.11: Measures Recommended to Improve the System (n=5

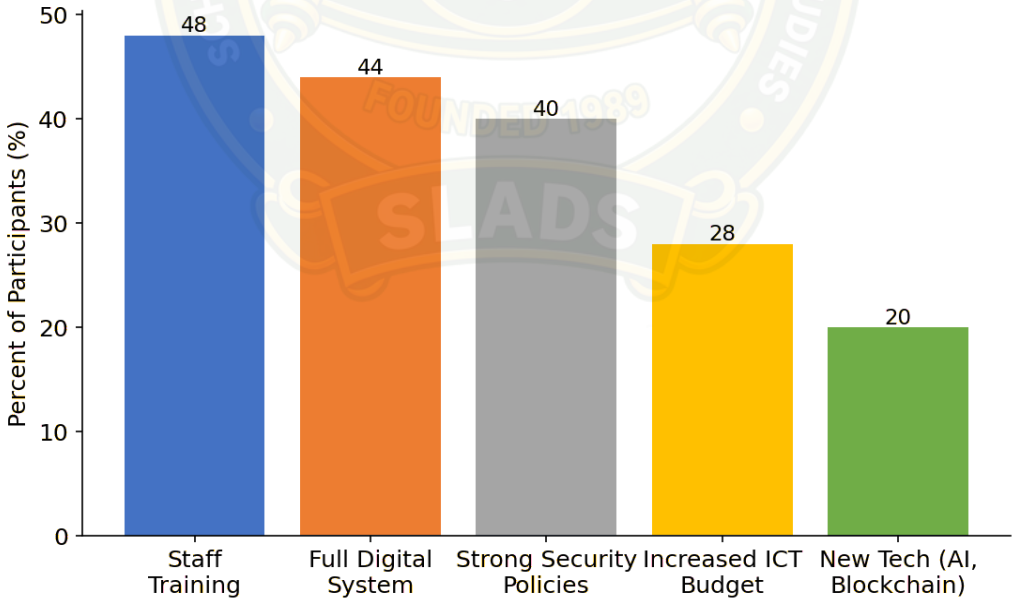


Figure 4.11: Measures Recommended to Improve the System (n=50)

Source: Field Study (2026)

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Figure shows that most participants 24 (48%) recommended staff training as the first measure for improving the system. The second most common solution was implementation of a full digital system (22 participants, 44%), followed by strong security policies (20 participants, 40%), increased ICT budget (14 participants, 28%), and adoption of new technologies such as Block chain and AI (10 participants, 20%).

It is worth observing that the ranking of recommended solutions mirrors, almost point for point, the ranking of challenges identified in Section 4.4.1: training addresses the training gap, full digitization addresses the hybrid-system problem, and stronger policy addresses incomplete-policy concerns. This internal consistency strengthens confidence in the validity of the survey instrument, since respondents were, in effect, proposing solutions proportionate to the problems they had separately reported

4.5.2 Interview Views on Improvement Measures

We need regular training on new digital systems. Many staff do not know how to use modern record systems well.

DIT needs a clear policy for managing digital records that follows international standards. Without a clear policy, we cannot be sure our data is safe.

These findings support the advice of Shinde and colleagues (2025) that AI technology and modern systems can greatly assist in strengthening digital records management. They also agree with the recommendations of Santillan-Lima and colleagues (2025) that compliance with international standards is an essential step in ensuring the long-term preservation of records.

Taken together, the quantitative ranking and the interview commentary point toward a two-track improvement path: an immediate, low-cost track built around staff training and formal policy adoption, both of which can begin without major capital outlay, and a medium-term, capital-intensive track built around full digitization, budget expansion, and emerging technologies such as block chain and AI, which require sustained institutional investment and, in most cases, external funding or government support. Sequencing the two tracks appropriately building the skills and policy foundation first, so that new technology is adopted

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

into an environment already capable of using it securely is likely to produce better outcomes than pursuing the more expensive technological upgrades in isolation.

4.6 Chapter Summary

This chapter presented the findings from 50 participants at DIT. The key findings are: most participants are male, well educated, and of working age; DIT still relies heavily on a hybrid system combining paper and digital records; access control and data backup are working reasonably well, but audit trails and encryption are weak; the biggest challenges are poor staff training, the hybrid system, and poor network connectivity; and the most recommended solution is staff training, followed by full digitization of records. The next chapter presents the summary, conclusion, and recommendations of this study.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.0 Introduction

This chapter gives a summary of the key findings of the study. It also presents the conclusion and recommendations. This study looked at how digital record management is used to strengthen data integrity and security at the Dar es Salaam Institute of Technology (DIT). The study used a mixed-methods approach, combining questionnaires and interviews, with a single case study design, to get detailed information from 50 participants.

5.1 Summary of Findings

5.1.1 Objective One: Digital Record Management Practices and Technologies

The study found that DIT still depends heavily on a hybrid system, where records are kept partly on paper and partly on computer. Only a small number of participants said they use a fully digital system. Many participants also said it is not always easy to find the records they need, mostly because of poor indexing. This shows that DIT is still in the early stages of moving to a fully digital records system.

5.1.2 Objective Two: Technical Controls and Policies

Access control and data backup were found to be working reasonably well. However, audit trails and encryption were found to be weak. Half of the participants were satisfied with the digital record system, while the other half were neutral or dissatisfied. Interviews showed that backups are not done on a regular schedule and that too many staff can access records without proper restriction.

5.1.3 Objective Three: Challenges Affecting Data Integrity and Security

The main challenges found were poor staff training, the hybrid system, poor network connectivity, cyber threats, low ICT budget, and incomplete policies. Interviews also raised the problem of unrestricted access to records, which increases the risk of insider threats, that is, harm caused by people who already work at the institution.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

5.1.4 Objective Four: Measures to Improve the System

Participants recommended staff training as the most important step, followed by full digitization of records, strong security policies, increased ICT budget, and the use of new technologies such as Block chain and AI. Records officers also said DIT needs clear policies that follow international standards.

5.2 Conclusion

Based on the findings, the study makes the following conclusions:

I. DIT still relies on a hybrid paper-and-digital system. This makes it harder to keep records safe and accurate, because two different systems must be managed and protected at the same time.

II. Some technical controls, such as access control and data backup, are working well. However, audit trails and encryption are weak. This means DIT cannot always prove who accessed or changed a record, which is a serious gap in data security.

III. Poor staff training is the biggest challenge facing DIT. Many staff do not have enough skills to use digital systems properly or to understand why data security matters.

IV. DIT does not yet fully follow international standards such as ISO 15489 and ISO 27001:2022, which set out the best ways to manage and protect records.

V. Tanzania has passed the Personal Data Protection Act (PDPA 2023), but institutions like DIT still face challenges putting it into practice, mainly due to a lack of resources, skills, and awareness.

Overall, the study shows that DIT needs a clear and complete plan to improve its digital record management system. This plan should focus on training staff, building stronger policies, and investing in better technology, so that data integrity and security can be fully protected.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

5.3 Recommendations

5.3.1 Recommendations for DIT

I. DIT should organize regular training, at least twice a year, for all staff who handle digital records. Training should cover how to use digital systems, data security basics, and international records management standards.

II. DIT should move towards a fully digital system step by step. This should start with turning old paper records into digital ones, to slowly reduce the problems caused by the hybrid system.

III. DIT should write and put in place clear data security policies that follow ISO 27001:2022 and ISO 15489 standards. These policies should clearly explain who can access records, how backups should be done, and what to do if there is a security problem.

IV. DIT should invest in better ICT infrastructure. This includes a stronger network, better record management software, and a backup system that runs regularly and automatically, instead of only when there is a problem.

V. DIT should set up a small team responsible for cybersecurity. This team should watch out for threats and respond quickly if something goes wrong.

VI. DIT should limit staff access to records based on their job. Only staff who need a record for their work should be able to open or edit it. This will reduce the risk of insider threats.

5.3.2 Recommendations for Government and Policy Makers

I. The Government of Tanzania should give clearer guidance to higher-learning institutions on how to follow the Personal Data Protection Act (PDPA 2023).

II. The Ministry of Education should set national standards for digital record management in higher-learning institutions. These standards should cover technical guidelines, security policies, and staff training requirements.

III. The Government should increase the ICT budget given to higher-learning institutions, so they can buy better systems and hire cybersecurity specialists.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

5.3.3 Recommendations for Further Research

I. Further research is needed on the use of Block chain technology in improving the integrity and security of digital records in higher-learning institutions in Tanzania.

II. A comparative study between DIT and other higher-learning institutions in Tanzania could shed further light on the overall state of digital records management in the country.

III. In-depth research is needed on how the Personal Data Protection Act (PDPA 2023) is being implemented in higher-learning institutions in Tanzania and the obstacles facing its implementation.

IV. Longitudinal research tracking DIT's progress after the implementation of the recommendations above would help establish which interventions training, policy, or technology investment contribute most to measurable improvements in data integrity and security.

V. Future work could also examine the cost-effectiveness of different digitization pathways, to give resource-constrained institutions like DIT an evidence base for sequencing their investments.

5.4 Contribution of the Study

This study has made a contribution in several respects. First, it has provided scholarly insight into the state of the digital records management system at a major higher-learning institution in Tanzania a situation that had not previously been studied in depth. Second, it has provided empirical evidence linking DRM practices with data integrity and security outcomes within the Tanzanian context, addressing an identified knowledge gap. Third, its findings can be used by policy makers in designing better strategies to improve digital records management in public institutions in Tanzania. Fourth, this study can serve as a foundation for further research in this important area. Fifth, by triangulating a 50-respondent structured survey with in-depth interviews of records officers, the study offers a methodological template that other researchers examining records management in similarly resourced institutions can replicate or adapt.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

5.5 Chapter Summary

This chapter presented a summary of the key research findings, the conclusion, and the recommendations arising from those findings. The study found that DIT faces significant challenges in implementing a robust digital records management system, including poor staff training, an inefficient hybrid system, weak technical controls, and growing cyber threats. The recommendations provided aim to address this situation in a strategic and sustainable manner, taking into account the available resources and the legal requirements governing data management in Tanzania. Implemented together, the recommendations in this chapter are intended to move DIT from its current transitional, hybrid state toward a fully digital, adequately governed, and internationally compliant records management environment.

5.6 Areas for Further Study

Based on the findings and conclusions of this research on This study looked at how digital record management is used to strengthen data integrity and security at the Dar es Salaam Institute of Technology (DIT), several areas for further study have been identified. These areas could contribute to a deeper understanding of the issues surrounding digital record management systems and provide valuable insights for future improvements:

I. **Impact of Digital Record Management on Accessibility and Efficiency**
   Further research could explore the **impact of digitization** on the accessibility and efficiency of digital record management systems. A study could assess how the transition from physical to digital record has affected user satisfaction, the speed of information retrieval, and overall record management practices. This would help gauge whether digitization truly enhances record management systems and its specific benefits to users.

II. **User Experience and Satisfaction with Different Record Management Systems**
   A comparative study could examine the **user experience** and **satisfaction** with different types of record management systems, such as physical vs. digital or automated vs. manual systems. This would help identify which systems are most effective in meeting user needs and providing timely, accurate, and relevant information. This research could also help understand the challenges users face in adapting to various archival technologies.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

III. **Effectiveness of Training Programs for Record Management Staff** given the importance of **staff training** in effective record management, further studies could focus on evaluating the effectiveness of **training programs** for record staff. Research could explore how training programs influence staff efficiency, user assistance, and overall satisfaction with record management services. The study could also assess the frequency and content of such programs, as well as the gaps in current staff knowledge and skills.

IV. **Record Management System Integration with Other Government Systems** another area for further study could be the **integration of the record management system** with other government systems and databases. Research could investigate how such integration can improve information accessibility, enhance data sharing between departments, and streamline overall administrative processes. This study could focus on the technical and operational challenges involved in such integrations.

V. **Long-Term Impact of Record Management System Updates on Decision Making** Future research could examine the **long-term impact of record Management system updates** on decision-making processes within the City Council. The study could focus on whether improved access to accurate and timely information leads to better policy-making, more informed decisions, and greater transparency in governance. This would be an important area of research for understanding how record management influence public administration and governance.

VI. **Perception of Record Management Systems among Different User Groups** A study could further explore how **different user groups** (e.g., researchers, government officials, and the general public) perceive and utilize record management systems. Understanding the needs, challenges, and preferences of these groups can help tailor record management systems to be more user-centered and responsive to diverse user demands.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

BIBLIOGRAPHY

Alhassan, M., & Adjei, E. (2022). Data integrity and security in digital record management systems. Journal of Information Science, 48(3), 312-328.

Asogwa, B. E., & Ezema, I. J. (2021). The challenges of digital record management in African public sector organizations. Records Management Journal, 31(2), 145-162.

Bell, E., Bryman, A., & Harley, B. (2019). Business research methods (5th ed.). Oxford University Press.

Chang'a, H., & Mwilongo, K. (2022). Factors influencing digital record sharing practices in Tanzanian public institutions. Tanzania Journal of Information Studies, 5(1), 45-62.

Corodata Team. (2025). Global data statistics 2024: The world of data generation and breaches. Corodata Publishing.

Creswell, J. W. (2012). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (4th ed.). Pearson.

Creswell, J. W., & Clark, V. L. P. (2017). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Crudu, R., & MoldStud Research Team. (2025). Cloud adoption trends 2025: Business perspectives. MoldStud Press.

Daniel, E. (2016). The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education. Journal of Education and Practice, 7(15), 91-100.

DPI Africa. (2024). Tanzania's digital economy strategy framework 2024-2034. Digital Public Infrastructure Africa.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

DPO Consulting. (2025). Data breach statistics report 2024: Global analysis. DPO Consulting Publications.

Duranti, L. (1997). Reliability and authenticity: The concepts and their implications. Archival Science, 1(1), 5-10.

Duranti, L., & Rogers, C. (2022). Trust in digital records: An increasingly cloudy legal area. Archival Science, 22(2), 165-185.

Ernest, J. (2025). Implementation challenges of Tanzania's Personal Data Protection Act 2023. East African Law Journal, 12(1), 78-95.

Gerring, J. (2023). Social science methodology: A unified framework (3rd ed.). Cambridge University Press.

Glenton, C., & Lewin, S. (2019). Qualitative evidence synthesis for health policy. SAGE Publications.

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.

Interpol. (2023). African cyber threat assessment report. International Criminal Police Organization.

ISMS.online. (2025). ISO 27001:2022 Annex A Control 5.33 implementation guide. ISMS.online.

ISO. (2016). ISO 15489-1:2016 Information and documentation -- Records management -- Part 1: Concepts and principles. International Organization for Standardization.

ISO. (2020). ISO 15489-1:2020 Information and documentation -- Records management -- Part 1: Concepts and principles (Revised ed.). International Organization for Standardization.

Kabir, S. M. S. (2016). Methods of data collection. In Basic guidelines for research (pp. 201-275). Book Zone Publication.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Kashaija, F. (2023). Digital transformation in Tanzanian public sector: Opportunities and challenges. Tanzania Journal of Development Studies, 20(2), 112-130.

Katuu, S. (2021). Digital records management in the public sector. Springer.

Kipande, J. (2025). Digital evidence management in Tanzanian courts: Integrity challenges. Journal of East African Legal Studies, 8(1), 34-52.

Kombo, D. K., & Tromp, D. L. A. (2006). Proposal and thesis writing: An introduction. Paulines Publications Africa.

Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd ed.). New Age International.

Kothari, C. R. (2019). Research methodology: Methods and techniques (4th ed.). New Age International.

Krishna, S. (2019). Research methodology and statistical analysis. Himalaya Publishing House.

Market Data Forecast. (2025). Africa cybersecurity market report 2024-2033. Market Data Forecast.

Matthew, D., & Liz, S. (2015). Case study research: Design and methods. SAGE Publications.

May, C. (2025). NARA's ISO 16363 self-assessment: Lessons for digital preservation. Digital Preservation Coalition Newsletter, 45, 12-18.

Mnjama, N. (2022). Electronic records management in East Africa: Progress and challenges. Journal of the South African Society of Archivists, 55, 78-94.

Mnjama, N., & Wamukoya, J. (2022). Records management practices in Tanzanian public universities. Mousaion, 40(2), 1-18.

Mwanga, E., & Kessy, A. (2022). Cybersecurity challenges in Tanzanian public institutions. Tanzania Journal of Information Technology, 7(1), 23-41.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Neuman, W. L. (2003). Social research methods: Qualitative and quantitative approaches (5th ed.). Allyn and Bacon.

Ngechu, M. (2006). Understanding the research process and methods. University of Nairobi Press.

Ngoepe, M., & Saurombe, A. (2022). Digital records management in Africa: A review of challenges and opportunities. Information Development, 38(3), 456-472.

Orodho, A. J. (2010). Techniques of writing research proposals and reports in education and social sciences. Maseno University Press.

Otuza, C., Okonkwo, C., & Nwosu, A. (2025). Blockchain adoption in Nigerian records management: Perspectives of IT specialists and records managers. African Journal of Library, Archives and Information Science, 35(1), 45-62.

Pieterse, J. (2025). The architecture gap: Reconciling records management and preservation systems. Archival Science, 25(2), 189-208.

Raj, A. (2005). Research methodology. APH Publishing.

RMFA. (2024). Annual report 2024: Promoting records management excellence in Africa. Records Management Foundation for Africa.

Rwagoshora, M. M. (2006). Guide to social science research. Mkuki na Nyota Publishers.

Safer-Panic, M. (2025). Digital evidence management systems in law enforcement. Journal of Digital Forensics, 18(2), 112-128.

Santillán-Lima, J., Díaz, P., Piccirilli, D., Guambo Vallejo, E., Duque-Vaca, M., & Molina-Granja, F. (2025). Digital preservation strategies in Latin America: A systematic review. Digital Library Perspectives, 41(1), 34-52.

Shinde, R., Kirstein, F., Ghosh, S., & Franks, P. (2025). Artificial intelligence applications in archival science: A systematic review. Journal of Archival Organization, 22(1), 1-24.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Taherdoost, H. (2018). Sampling methods in research methodology. International Journal of Academic Research in Management, 7(2), 18-27.

Tech Hive Advisory. (2024). Africa data protection landscape report 2024. Tech Hive Advisory.

Tencent Cloud. (2025). Best practices for data backup security. Tencent Cloud Documentation.

The Citizen. (2025, January 15). Tanzania positions data as national asset for economic growth. The Citizen, p. 5.

URT. (2023). National ICT policy framework 2023. United Republic of Tanzania, Ministry of Communication and Information Technology.

Verma, J. P., Abdel-Salam, G., & Verma, P. (2017). Testing statistical assumptions in research. Wiley.

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

REFERENCES

Alhassan, M., & Adjei, E. (2022). Data integrity and security in digital record management systems. Journal of Information Science, 48(3), 312-328.

Asogwa, B. E., & Ezema, I. J. (2021). The challenges of digital record management in African public sector organizations. Records Management Journal, 31(2), 145-162.

Bell, E., Bryman, A., & Harley, B. (2019). Business research methods (5th ed.). Oxford University Press.

Chang'a, H., & Mwilongo, K. (2022). Factors influencing digital record sharing practices in Tanzanian public institutions. Tanzania Journal of Information Studies, 5(1), 45-62.

Corodata Team. (2025). Global data statistics 2024: The world of data generation and breaches. Corodata Publishing.

Creswell, J. W. (2012). Educational research: Planning, conducting, and evaluating quantitative and qualitative research (4th ed.). Pearson.

Creswell, J. W., & Clark, V. L. P. (2017). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Crudu, R., & MoldStud Research Team. (2025). Cloud adoption trends 2025: Business perspectives. MoldStud Press.

Daniel, E. (2016). The usefulness of qualitative and quantitative approaches and methods in researching problem-solving ability in science education. Journal of Education and Practice, 7(15), 91-100.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

DPI Africa. (2024). Tanzania's digital economy strategy framework 2024-2034. Digital Public Infrastructure Africa.

DPO Consulting. (2025). Data breach statistics report 2024: Global analysis. DPO Consulting Publications.

Duranti, L. (1997). Reliability and authenticity: The concepts and their implications. Archival Science, 1(1), 5-10.

Duranti, L., & Rogers, C. (2022). Trust in digital records: An increasingly cloudy legal area. Archival Science, 22(2), 165-185.

Ernest, J. (2025). Implementation challenges of Tanzania's Personal Data Protection Act 2023. East African Law Journal, 12(1), 78-95.

Gerring, J. (2023). Social science methodology: A unified framework (3rd ed.). Cambridge University Press.

Glenton, C., & Lewin, S. (2019). Qualitative evidence synthesis for health policy. SAGE Publications.

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.

Interpol. (2023). African cyber threat assessment report. International Criminal Police Organization.

ISMS.online. (2025). ISO 27001:2022 Annex A Control 5.33 implementation guide. ISMS.online.

ISO. (2016). ISO 15489-1:2016 Information and documentation -- Records management -- Part 1: Concepts and principles. International Organization for Standardization.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

ISO. (2020). ISO 15489-1:2020 Information and documentation -- Records management -- Part 1: Concepts and principles (Revised ed.). International Organization for Standardization.

Kabir, S. M. S. (2016). Methods of data collection. In Basic guidelines for research (pp. 201-275). Book Zone Publication.

Kashaija, F. (2023). Digital transformation in Tanzanian public sector: Opportunities and challenges. Tanzania Journal of Development Studies, 20(2), 112-130.

Katuu, S. (2021). Digital records management in the public sector. Springer.

Kombo, D. K., & Tromp, D. L. A. (2006). Proposal and thesis writing: An introduction. Paulines Publications Africa.

Kothari, C. R. (2004). Research methodology: Methods and techniques (2nd ed.). New Age International.

Kothari, C. R. (2019). Research methodology: Methods and techniques (4th ed.). New Age International.

Krishna, S. (2019). Research methodology and statistical analysis. Himalaya Publishing House.

Market Data Forecast. (2025). Africa cybersecurity market report 2024-2033. Market Data Forecast.

Matthew, D., & Liz, S. (2015). Case study research: Design and methods. SAGE Publications.

May, C. (2025). NARA's ISO 16363 self-assessment: Lessons for digital preservation. Digital Preservation Coalition Newsletter, 45, 12-18.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Mnjama, N. (2022). Electronic records management in East Africa: Progress and challenges. Journal of the South African Society of Archivists, 55, 78-94.

Mnjama, N., & Wamukoya, J. (2022). Records management practices in Tanzanian public universities. Mousaion, 40(2), 1-18.

Mwanga, E., & Kessy, A. (2022). Cybersecurity challenges in Tanzanian public institutions. Tanzania Journal of Information Technology, 7(1), 23-41.

Neuman, W. L. (2003). Social research methods: Qualitative and quantitative approaches (5th ed.). Allyn and Bacon.

Ngechu, M. (2006). Understanding the research process and methods. University of Nairobi Press.

Ngoepe, M., & Saurombe, A. (2022). Digital records management in Africa: A review of challenges and opportunities. Information Development, 38(3), 456-472.

Orodho, A. J. (2010). Techniques of writing research proposals and reports in education and social sciences. Maseno University Press.

Pieterse, J. (2025). The architecture gap: Reconciling records management and preservation systems. Archival Science, 25(2), 189-208.

Raj, A. (2005). Research methodology. APH Publishing.

RMFA. (2024). Annual report 2024: Promoting records management excellence in Africa. Records Management Foundation for Africa.

Rwagoshora, M. M. (2006). Guide to social science research. Mkuki na Nyota Publishers.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

Santillán-Lima, J., Díaz, P., Piccirilli, D., Guambo Vallejo, E., Duque-Vaca, M., & Molina-Granja, F. (2025). Digital preservation strategies in Latin America: A systematic review. Digital Library Perspectives, 41(1), 34-52.

Shinde, R., Kirstein, F., Ghosh, S., & Franks, P. (2025). Artificial intelligence applications in archival science: A systematic review. Journal of Archival Organization, 22(1), 1-24.

Taherdoost, H. (2018). Sampling methods in research methodology. International Journal of Academic Research in Management, 7(2), 18-27.

Tech Hive Advisory. (2024). Africa data protection landscape report 2024. Tech Hive Advisory.

Tencent Cloud. (2025). Best practices for data backup security. Tencent Cloud Documentation.

The Citizen. (2025, January 15). Tanzania positions data as national asset for economic growth. The Citizen, p. 5.

URT. (2023). National ICT policy framework 2023. United Republic of Tanzania, Ministry of Communication and Information Technology.

Verma, J. P., Abdel-Salam, G., & Verma, P. (2017). Testing statistical assumptions in research. Wiley.

Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper and Row.

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

APPENDIXI

DETAILEDRESEARCHBUDGET

	ACTIVITY	COSTANALYSIS	TOTALCOST
1	Transport	From home to Dar es Salaam Institute of Technology (DI	=35,000/=
2	Stationary	Ruledpaper1ream= Pen, Pencils, Ruler, Rubber, Stapler & Notebook =	=25,000/=
3	Secretarial service	Typing, photocopy and printing	=100,000/=
4	Binding	Hardcover2x2@2000 Softcaver2x2@500andCD	=150,000/=
5	Substances Allowance	Meal per day and accommodation	=150,000/=
	TOTAL		**= 460,000**/=

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

APPENDIXII

TIMESCHEDULE

ACTIVITIES	1st **MONTH**	2nd **MONTH**	3rd **MONTH**	4th **MONTH**	5th **MONTH**	6th **MONTH**
Report at the study area and get familiarization						
Distribution questionnaire interviewing respondents						
Observation situation and collect questionnaire and analysis						
Data interpretation report writing.						

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

APPENDIXIII

QUESTIONNAIRES GUID FOR REGISTRY STAFF RESIDENTS

My name is **RAMADHAN AHMED MBWILO** the student from School of Library, Archives and Documentation Studies (SLADS), Pursuing Ordinary Diploma in Records and archive Management Studies. I am undertaking the research titled *"**An Assessment on of the use of digital record management on data integrity and security a case study at dar es salaam institute of technology (d.i.t)**"*. Kindly, I'm requesting your corporation to fill my questionnaire. All responses that will be given will be treated with high privacy and confidentiality and thus will be applied for only academic purpose not otherwise.

A. DEMOGRAPHICINFORMATION

1. What is your gender?

a. Male ()
b. Female ()

2. What is your highest level of education?

a. PhD ()
b. Master's Degree ()
c. Bachelor Degree ()
d. Diploma ()
e. Certificate ()

3. Which age categories describe your age?

a. 20-28 ()
b. 29-34 ()
c. 35-44 ()
d. 45andabove ()

4. How satisfied are you with the ability of the archival system to provide the information you need?

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

a. Very satisfied ()
b. Satisfied ()
c. Neutral ()
d. Dissatisfied ()
e. Very dissatisfied ()

5. How relevant is the information retrieved from the digital record system to your needs?
    a. Highly relevant ()
    b. Relevant ()
    c. Neutral ()
    d. Irrelevant ()
    e. High irrelevant ()
6. How well does the registry meet your expectations in terms of providing accurate and up-to-date information?

    a. Excellent ()
    b. Good ()
    c. Fair ()
    d. Poor ()
    e. Very poor ()

7. How easy is it to locate record materials when you need them?

    a. Very easy ()
    b. Easy ()
    c. Neutral ()
    d. Difficult ()
    e. Very difficult ()

8. What is your primary method of accessing document?

a. online access ()
b. Physical visits ()

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

c. Both ()

d. Others (please specify) ()

9. What are the most common challenges you face when accessing records?
    a. Lack of proper indexing ()
    b. Outdated systems ()
    c. Limited accessibility ()
    d. Poor staff support ()
    e. Others (please specify) ()
10. Do you think what should be done to address the challenges that hinder accessibility of registry materials……
……?

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

APPENDIXIV

INTERVIEW GUIDE QUESTIONS FOR RECORD OFFICERS

i. Can you describe how the archival system is structured to meet users 'information needs?
ii. How do you measure the effectiveness of the archival system in providing relevant information to users?
iii. How often do users request information that is not available in the archives?
iv. What steps do you take to ensure the archival materials are up-to-date and relevant for users?
v. How do you handle cases where users are dissatisfied with the information provided from the archives?
vi. What methods do you use to assess whether the archives are meeting users ‘information needs?
vii. In your experience, what types of information do users most frequently request from the archives?
viii. What challenges do you face in ensuring the archival system effectively meets users ‘information needs?

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz

THE UNITED REPUBLIC OF TANZANIA

MINISTRY OF
EDUCATION, SCIENCE AND TECHNOLOGY

DAR ES SALAAM INSTITUTE OF TECHNOLOGY

Ref. No: AB.83/284/01/139 27th March 2026

Student Name: Ramadhan Ahmad Mbwilo
School of Library, Archives and Documentation Studies (SLADS),
Ukuni, Block S, Plot No.96,
P. O. BOX 227, **BAGAMOYO**.

Re: Authorisation for Data Collection at Dar es Salaam Institute of Technology (DIT)

Reference is made to SLABS letter (Ref No DA.201/457/Vol/1/20, dated 9 March 2026), requesting permission for you to conduct data collection at DIT for your diploma project titled "Assessment of the Use of Digital Records Management on Data Integrity and Security- A case Study of the Dar es Salaam Institute of Technology".

2. I am pleased to inform you that you have been granted permission to conduct data collection at DIT for your project from 6th April to 6th May 2026.

3. Kindly note that all the data that will be collected from DIT will have to be treated with the highest level of confidentiality and used exclusively for academic purposes.

5. If the results are to be published on any online platform, any text in which our Institute is mentioned must first be reviewed and approved by our Institute prior to publication.

6. Please present this letter to any Department Heads or respondents as proof of authorization while on campus.

7. If you have any questions or require further assistance during your time at DIT, please contact Dr. Ahab Ndabigaye, the Coordinator for Research, Publication and Innovation. He can be reached through his email ahab.ndabigaye@dit.ac.tz or mobile phone number 0775294539.

8. Thank you.

Dr. Ahab Ndabigaye
FOR RECTOR

Junction of Morogoro Road and Bibi Titi Mohamed, P.O. Box 2958, Dar es Salaam- TANZANIA
Tel: +255 22 2150174, Fax: +255 22 2152504, Email: drcp@dit.ac.tz, Website: www.dit.ac.tz

SLADS Research Hub · SLADS/2026/00019 · repository.slads.sc.tz