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

RESEARCH REPORT ON

AN ASSESSMENT ON GOVERNMENT RECORDS SECURITY CONTROLS ON ENHANCING CONFIDENTIALITY TO CUSTOMER RECORDS: CASE STUDY AT TANZANIA REVENUER AUTHORITY (TRA), KINONDONI REGION.

JONATHAN JACKSON JOHN.

A Research Report Submitted to the School of Library, Archives and Documentation Studies (SLADS) seeking Approval to Undertake a Research Study for Partial Fulfillment for the Award of Ordinary Diploma in Records and archive management.

SUPERVISED BY IBRAHIM A. JOJO.

2025/2026

SLADS Research Hub · SLADS/2026/00046 · 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) a research report titled: "An Assessment on Government Records Security Controls on Enhancing Confidentiality of Customer Records: A Case Study at Tanzania Revenue Authority (TRA), Kinondoni Region", in partial fulfillment of the requirements for the award of Ordinary Diploma in Records and Archives Management.

.....

Ibrahim A. Jojo

(Supervisor)

Date: .....

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

DECLARATION AND COPYRIGHT.

I, Jonathan Jackson John, declare that this research report is my own original work and that it has not been presented and will not be presented to any other institution for a similar or any other academic award.

Signature: .....

Date: .....

© JONATHAN. J (2026)

This report is copyright material protected under the Berne Convention, the Copyright Act of 1999, and other international and national enactments, in that behalf, 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 an acknowledgement, without the written permission of the School of Library, Archives and Documentation Studies (SLADS) on behalf of the author.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

ACKNOWLEDGEMENT.

I express my deepest gratitude to Almighty God for the strength, guidance, and good health provided throughout the period of this academic journey.

My sincere thanks go to my research supervisor, **SIR. IBRAHIM A. JOJO**, for his invaluable guidance, constructive feedback, and continuous support during the conceptualization and completion of this research report.

I extend my appreciation to the management and staff of the Tanzania Revenue Authority (TRA), Kinondoni Regional Office, for granting permission and providing cooperation during data collection. My appreciation further extends to my fellow students and colleagues for their moral support, encouragement, and constructive discussions throughout this study. Finally, I thank my family and peers at the School of Library, Archives and Documentation Studies (SLADS) for their encouragement and support.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

DEDICATION.

This research report is dedicated to my beloved family for their unwavering support, continuous sacrifices, and encouragement throughout my academic pursuits.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

ABBREVIATIONS.

ARSO	-	African Regional Organization for Standardization
CCTV	-	Closed-Circuit Television
CVI	-	Content Validity Index
DPCT	-	Data Protection Commissioner of Tanzania
EAC	-	East African Community
GDPR	-	General Data Protection Regulation
ICA	-	International Council on Archives
ICT	-	Information and Communications Technology
ISO	-	International Organization for Standardization
KRA	-	Kenya Revenue Authority
MFA	-	Multi-Factor Authentication
NDA	-	Non-Disclosure Agreement
PDPC	-	Personal Data Protection Commission
RAM	-	Records and Archives Management
RBAC	-	Role-Based Access Control
SLADS	-	School of Library, Archives and Documentation Studies
SPSS	-	Statistical Package for the Social Sciences
TIN	-	Taxpayer Identification Number
TRA	-	Tanzania Revenue Authority
URA	-	Uganda Revenue Authority

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

ABSTRACT.

This study assessed government records security controls in enhancing the confidentiality of customer records, using the Tanzania Revenue Authority (TRA), Kinondoni Regional Office, as a case study. The research was guided by three specific objectives: examining current physical security measures, determining challenges facing security controls, and identifying possible solutions to protect customer record confidentiality. A descriptive cross-sectional research design employing a mixed-methods approach was adopted. The target population comprised 264 employees, from which a sample size of 159 respondents was derived using Slovin's formula. Data collection was executed through structured questionnaires, semi-structured key informant interviews, and documentary observation. Quantitative data were analyzed using descriptive statistics via SPSS version 25.0, while qualitative data underwent thematic analysis. The findings revealed strong structural perimeter controls (server rooms locked, mean = 4.34) and effective role-based access control within the IT system (mean = 4.01). However, critical vulnerabilities were identified, including the absence of automated biometric access tracking (mean = 3.12) and the lack of mandatory Multi-Factor Authentication (MFA) (mean = 2.52). Operational challenges were predominantly driven by power outages and network instability (mean = 4.10), which forced manual, paper-based workarounds that bypass digital audit logs. Infrequent staff training on data privacy (mean = 2.93) also exposed the organization to human-error security risks. The study concludes that while foundational perimeter and role isolation controls exist, operational and technical gaps hinder complete alignment with the Personal Data Protection Act No. 11 of 2022 and ISO/IEC 27001:2022 standards. It is recommended that TRA deploy mandatory MFA, integrate biometric tracking, establish dedicated solar backup links to eliminate manual workarounds, and conduct mandatory quarterly data privacy training for all staff.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

TABLES OF CONTENTS

CERTIFICATION. i
DECLARATION AND COPYRIGHT. ii
ACKNOWLEDGEMENT. iii
DEDICATION. iv
ABBREVIATIONS. v
ABSTRACT. vi
LIST OF TABLES. x
LIST OF FIGURES xi
CHAPTER ONE 1
1.0 INTRODUCTION. 1
1.1 Background of the study. 1
1.2 Statement of the problem. 3
1.3 General objective. 4
1.4 Specific objective. 4
1.5 Research question 4
1.6 Significance of the study. 4
1.7 Definition of key concept. 6
CHAPTER TWO 7
2.0 LITERATURE REVIEW 7
2.1 Customer records, confidentiality and security measures concepts. 7
2.2 Physical security measures and confidentiality. 8
2.3 Challenges facing security controls in tax administrations. 8
2.4 The possible solutions to problems identified in the security controls for protecting the confidentiality of customer records. 9
2.5 Legal and regulatory framework. 9
2.6 Research gap. 9
CHAPTER THREE 11
3.0 RESEARCH METHODOLOGY 11

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

3.1 Research design. 11
3.2 Study area. 11
3.3 Study population. 12
3.4 Sample size 13
3.5 Sampling procedure. 14
3.6 Data collection methods. 14
3.6.1 Primary data. 14
3.6.2 Secondary data. 16
3.7 Data analysis. 16
3.7.1 Quantitative data analysis 17
3.7.2 Qualitative data analysis. 18
3.8 Validity and reliability of research instruments. 19
3.8.1 Validity. 19
3.8.2 Reliability. 20
3.9 Ethical considerations. 20
CHAPTER FOUR 22
4.0 DATA PRESENTATION, ANALYSIS, AND DISCUSSION 22
4.1 Introduction 22
4.2 Section A: Demographic information of respondents. 23
A.1 Gender distribution. 23
A.2 Age group distribution. 24
A.3 Educational qualifications. 25
A.4 Time of work experience 26
A.5 Job Categories 27
4.3 Section B: Physical security measures and confidentiality. 28
4.4 Section C: Technical security measures and system controls. 31
4.5 Section D: Administrative security measures and policy compliance. 33
4.6 Section E: Challenges facing security controls in records management 35
4.7 Section F: Possible solutions to strengthen security controls 38

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

4.8 Summary of the chapter. 39
CHAPTER FIVE 41
5.0 SUMMARY OF FINDINGS, CONCLUSION, AND RECOMMENDATIONS. 41
5.1 Introduction. 41
5.2 Summary of main findings. 41
5.3 Conclusion. 42
5.4 Recommendations. 43
REFERENCES: 44
APPENDEX I. 49
QUESTIONNAIRE FOR STAFF. 49
APPENDEX III. 53
TIME SCHEDULE SHOWING. 53
APPENDEX IV 54
RESEARCH REPORT BUDGETING. 54
APPENDIX V 55
VERICATION LETTER FOR DATA COLLECTION 55

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

LIST OF TABLES.

Table 4.1: Distribution of respondents by gender (n=159)…….23

Table 4.2: Distribution of respondents by age group (n=159)……24

Table 4.3: Distribution of educational qualifications (n=159)……25

Table 4.4: Distribution by work experience (n=159)…….27

Table 4.5: Distribution of respondents by job category (n=159)…….28

Table 4.6: Physical security statement evaluation matrix (n=159)……29

Table 4.7: Technical security control evaluation matrix (n=159)……31

Table 4.8: Administrative security measures evaluation matrix (n=159)……33

Table 4.9: Security control challenge evaluation matrix (n=159)……35

Table 4.10: Recommended solution statement evaluation matrix (n=159)……38

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

LIST OF FIGURES

Figure 4.1: Distribution of respondents by gender (n=159)……24

Figure 4.2: Distribution of respondents by age group (n=159)…….25

Figure 4.3: Distribution of educational qualifications (n=159)…….26

Figure 4.4: Distribution by work experience (n=159)……27

Figure 4.5: Physical security statement evaluation matrix (n=159)……29

Figure 4.6: Insufficient budget as a major challenge (n=159)…….37

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

CHAPTER ONE.

1.0 INTRODUCTION.

1.1 Background of the study.

Globally, organizations are confronting a rising incidence of data breaches, prompting a widespread adoption of advanced encryption and stringent access controls to maintain public trust (Standard, 2022). In the modern digital countryside, the management of records has transitioned from traditional physical ledgers to sophisticated electronic systems, significantly increasing risks to data privacy. The security of customer records is underpinned by the core principles of confidentiality, integrity, and availability, as delineated in international standards such as ISO/IEC 27001:2022. Robust security measures, on all sides of physical, technical, and administrative controls, are vital for safeguarding sensitive information

Within the African context, this digital transformation is pushed by rapid technological adoption across the continent, yet it has heightened vulnerabilities, particularly in sectors managing sensitive customer data like taxation and revenue collection. Loyalty to confidentiality, integrity, and availability remains top, supported by standards like ISO/IEC 27001:2022. Effective controls include physical safeguards such as secure storage facilities, technical measures like encryption and firewalls, and administrative protocols encompassing access policies and training to mitigate breaches (ISO, 2022). Yet, Africa contends with distinctive challenges, including inconsistent infrastructure, resource limitations, and a production of cyber threats targeting governmental entities, fostering a continental imperative for fortified data protection frameworks (ARSO, 2020).

In the East African community (EAC), tax administrations such as the Kenya revenue authority (KRA) and the Uganda revenue authority (URA) have emerged as prime targets for cyberattacks and unauthorized data disclosures. Regional analyses underscore that while technological adoption is pervasive, human factors and deficient records management persist as critical vulnerabilities (Mwencha, 2020). So, there is a concerted

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

regional effort to establish uniform data protection protocols to secure tax records, which constitute vital national assets.

Tanzania has demonstrated substantial progress in modernizing its records and archives management framework, as evidenced by the national records and archives management Act, which provides a systematic approach to controlling public records (ICA, 2017). An essential advancement is the performing of the personal data protection Act No. 11 of 2022, mandating that all data collectors and processors, including the Tanzania Revenue Authority (TRA), implement appropriate technical and organizational measures to shield personal data from unauthorized access, loss, or destruction (DPCT, 2023). This legislation marks a paradigm shift from discretionary compliance to obligatory legal loyalty, ensuring the confidentiality of customer records.

The Tanzania Revenue Authority (TRA) oversees limitless quantities of sensitive financial and personal data. The Kinondoni region, a center of economic activity in Tanzania, manages a large volume of taxpayer records. Since 2015, TRA has pursued digitalization through initiatives like the integrated tax management system (High Tax). Aside these advancements, questions continue regarding the efficacy of security controls at the regional level, especially in Kinondoni. Assessing these controls against the 2022 Act's requirements is essential to uphold taxpayer confidentiality amid the shift to fully automated records management (TRA Seventh Corporate Plan, 2023).

Confidentiality, integrity, and availability form the nucleus of this inquiry. With an emphasis on confidentiality standards (ISO, 2022), safeguarding taxpayer data rise above simple operational choice; it is now a constitutional imperative for TRA. Focusing on Kinondoni is strategically fitting, as its high record volume presents a rigorous test for TRA's security protocols, potentially absent in less active regions. Practical evidence on TRA Kinondoni's adaptation of organizational and technical measures to make straight with the personal data protection Act of 2022 remains infrequent (United Republic of Tanzania, 2022). While technical controls such as encryption are operational, research highlights the human element (Mwencha, 2020), revealing deficiencies in administrative

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

controls like staff training, ethical standards, and internal access hierarchies at the regional tier.

To strengthen confidentiality, this study classifies controls into three categories: technical like encryption, passwords, and firewalls within the high tax system, physical like restricted access to server rooms and filing cabinets in Kinondoni and administrative like training, non-disclosure agreements, and personal data protection policies (ISO, 2022). Adopting an evaluative and proactive methodology, the study seeks to foster a privacy by design code by evaluating existing controls against emergent legal levels (ICA, 2016).

1.2 Statement of the problem.

The Tanzania revenue authority (TRA) faces ongoing risks to its taxpayer record protection because the organization has not fully adopted digital record systems which include the integrated tax management system high tax and other advanced digital security solutions. The Tanzania revenue authority (TRA) has developed multiple security measures yet its increased advancement into digital platforms has led to greater priority being given to fast revenue collection than to establishing solid data protection systems (TRA Seventh Corporate Plan, 2023).

The existing security systems fail to meet the security demands set by personal data protection Act No. 11 of 2022. The system has established technical controls through encryption and firewalls but the organization remains exposed to threats which stem from human errors and administrative failures (Mwencha,2020). The Kinondoni area becomes a major target for unauthorized access and internal data leaks because its active zones handle large amounts of sensitive financial information, which could damage public confidence and result in serious legal consequences according to the 2022 Act.

The current physical, technical and administrative controls of these systems lack experiential proof representing their ability to fulfill with privacy by design requirements under existing legal standards. The Tanzania revenuer authority (TRA) will face dual pressures of national law destructions and sensitive taxpayer information exposure if it fails to perform complete assessment of it is security control.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

1.3 General objective.

To assess the government records security controls to enhance confidentiality of customer records.

1.4 Specific objective.

1. To examine the current physical security measures on enhancing the confidentiality of customer records.

2. To determine the challenges facing security controls of customer records to ensure confidentiality.

3. To identify possible solutions to security controls for protecting the confidentiality of customer records.

1.5 Research question.

1.What are the current physical security measures on enhancing the confidentiality of customer records?

2. What challenges facing security controls of customer records to ensure confidentiality?

3. What are the possible solutions can be recommended to strengthen security control to protect the confidentiality of customer records?

1.6 Significance of the study.

The significance of this study, lies in its practical and theoretical contributions to information governance, records management, and data protection within the Tanzanian public sector. By evaluating the position of TRA's internal security protocols with the personal data protection Act No. 11 of 2022, the research provides actionable insights for mitigating data breach risks, thereby preventing legal penalties and reputational damage. Drawing on established literature, such as Ndenje (2015), who emphasizes robust records management as a strategic resource for government accountability, the study underscores the importance of secure handling of sensitive taxpayer data in fostering institutional integrity.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

For records and archives management consultants, the research offers professional guidance on transitioning from physical to electronic records security. It demonstrates the application of ISO/IEC 27001:2022 standards in a localized tax administration context, equipping practitioners with tools to maintain confidentiality, integrity, and availability (CIA) throughout the record lifecycle. Argues, records managers must evolve into digital risk managers to address emerging cyber threats, and this study provides empirical evidence to support that evolution (Wamukoya, 2019).

To policymakers and the government, the findings serve as an evaluative framework for assessing the implementation of national data protection laws at the regional level. Insights from the Kinondoni case study can inform refinements to guidelines across other public institutions, enhancing the effectiveness of electronic governance. This places of interest that public trust in the handling of sensitive information is crucial for the success of electronic government initiatives (Wamukoya,2019).

For taxpayers and the general public, the study advocates for stronger security controls to protect personal and financial data, thereby safeguarding taxpayer rights. By promoting a secure environment, it contributes to building public trust, which is essential for voluntary tax compliance and the realization of objectives outlined (TRA Seventh Corporate Plan, 2023).

Initially, to the academic community and future researchers, this study develops the body of knowledge on information governance and records management in Africa. It provides empirical evidence on the effectiveness of security controls against cyber threats, addressing the dynamic challenges of digital records management. Continuous research is vital in this field, and this work offers a foundation for further investigations into data protection practices in developing contexts. Overall, the research bridges theory and practice, informing policy, professional practice, and scholarly discourse while promoting accountability and trust in public institutions (Ambira,2017).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

1.7 Definition of key concept.

Assessment; The systematic process of documenting and using empirical data on the knowledge, skill, attitudes, and beliefs to refine programs and improve student learning or system performance (Wamukoya, 2019).

Confidentiality of customer records; The legal and technical assurance that sensitive taxpayer data handled by the tax authority is protected from unauthorized access, loss, or disclosure in accordance with data protection principles (United Republic of Tanzania, 2022).

Confidentiality; The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27001:2022).

Customer; An individual or legal entity, commonly referred to as a taxpayer, who is registered with the tax authority and fulfills statutory obligations regarding revenue and taxation (TRA, 2023).

Customers records; Any information, regardless of form or medium, created or received by the tax authority that documents the financial transactions, tax returns, and personal identity of a taxpayer (Mwencha, 2020).

Records; Information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business (United Republic of Tanzania, 2022).

Security control; The management, operational, and technical safeguards or counter-measures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (ISO/IEC 27001:2022).

Security; The state of being protected against the unauthorized use of information, especially electronic data, or the measures taken to achieve this (Luthuli, 2017).

Tanzania revenuer authority (TRA); A semi-autonomous government agency responsible for managing the assessment, collection, and accounting of all central government revenue in Tanzania (TRA, 2023).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

CHAPTER TWO.

2.0 LITERATURE REVIEW

2.1 Customer records, confidentiality and security measures concepts.

Various studies defined and explained in different ways concepts of customer records, confidentiality and security measures. The management of customer records has evolved significantly in the digital era, transitioning from physical filing systems to complex digital repositories. In the field of records and archives management (RAM), Customer records are documents that show all transactions and communications between an organization and its clients. Records must be authentic, reliable, and well-managed throughout their entire lifecycle (ISO, 2016). Scholars like (McKemmish and Yates, 2019) emphasize that customer records are not just paperwork, they are strategic assets that support organizational memory and accountability. Confidentiality means protecting customer information from unauthorized access or misuse. GDPR requires organizations to ensure personal data is securely processed. Confidentiality is both a legal and ethical obligation, records managers must protect the privacy of every individual whose information they hold (Shepherd & Yeo, 2003) and (Jimerson, 2009). Security measures are the tools and systems used to keep records safe. ISO/IEC 27001 provides the global standard for information security, covering technical controls like encryption and access management. Role based access control (RBAC) ensures only authorized staff can access specific records. Emerging technologies like blockchain are also being explored to prevent tampering and ensure transparency.

The literature present indicates a clear consensus: customer records, confidentiality, and security measures are inextricably linked. (ISO, 2016) and (GDPR, 2016) provide the foundational standards, while scholars like (McKemmish, 2019) and (Yates, 2019) provide the theoretical framework for implementation. Security is not only a technical issue but a governance issue requiring a complete approach. As organizations continue to digitize, the integration of robust security measures with ethical confidentiality practices will remain the foundation of effective records and archives management.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

2.2 Physical security measures and confidentiality.

Physical security is the first line of defense in records management. An argues that even in a digital age, the physicality of infrastructure like servers, data centers, and terminals remains a weakness (Ambira, 2017). Within access control the biometric systems and restricted zones are essential for protecting sensitive government archives, (Luthuli, 2017). For an organization like TRA, physical barriers prevent unauthorized individuals from gaining direct access to hardware that stores customer data. Within environmental controls the current record and archive management (RAM) standards suggest that physical security also involves protection against environmental hazards like fire, floods, which could lead to data loss (ISO, 2022).

2.3 Challenges facing security controls in tax administrations.

Despite the advancement of systems like high tax, several sprints persevere in maintaining record confidentiality. Within the human factor and insider threat the identifies that the greatest threat to electronic records in East Africa is not external hacking, but internal insider threats (Mwencha, 2020). This includes forgetfulness, lack of ethics, or intentional data leaks by staff. In technological obsolescence the notes that many African public sectors struggle with heritage systems that are no longer compatible with modern encryption standards, making them easy targets for cyber-attacks (Wamukoya, 2019). At regulatory gaps while Tanzania has the personal data protection Act No. 11 of 2022, the challenge lies in the operationalization of the law at the regional level, where resources may be thinner than at the headquarters (DPCT, 2023). Infrastructure and resources in the African context, infrastructure challenges are marked. consistent power supply and internet connectivity in East African regions can force organizations to sidestep security protocols or depend on insecure workarounds (ARSO, 2020). Furthermore, resource limitations often prevent the adoption of advanced security technologies. In Tanzania, while the TRA has modernized, regional disparities exist. The acknowledges that while revenue collection is prioritized, the budget allocation for robust data protection systems in regional offices may interval behind (TRA Seventh Corporate Plan, 2023).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

2.4 The possible solutions to problems identified in the security controls for protecting the confidentiality of customer records.

To mitigate the risks mentioned above, researchers suggest a multi-layered approach, privacy by design this approach suggests that privacy and data protection should be integrated into the system's development from the very beginning, rather than added as an afterthought (ICA, 2016). Continuous capacity building asserts that regular training for records officers on data ethics and cyber-hygiene is the most effective administrative control to prevent human error (Ndenje, 2015). Encryption and multi-factor authentication (MFA) from a technical standpoint, implementing robust encryption for data at rest and in transfer is inflexible for modern tax authorities (Standard, 2022).

2.5 Legal and regulatory framework.

The study is deeply influenced by the legal site governing data protection and records management in Tanzania. The personal data protection Act no. 11 of 2022 this Act is the foundation of data privacy in Tanzania. It mandates that all data collectors and processors, including the TRA, implement appropriate technical and organizational measures to shield personal data (DPCT, 2023). It shifts the paradigm from voluntary compliance to mandatory legal obligation, ensuring the confidentiality of customer records. The national records and archives management Act passed to provide a systematic approach to controlling public records, this Act supports the legal framework for managing taxpayer data (ICA, 2017). It requires public institutions to maintain records as evidence and assets, demanding secure handling. International standards provide the international standard for information security management. It defines the core principles of confidentiality, integrity, and availability (CIA). Adherence to this standard is crucial for TRA to maintain public trust and align with global best practices (Standard, 2022).

2.6 Research gap.

The study shows that there is lack of specific research on how the Tanzania revenuer authority Kinondoni region protects the confidentiality of customer records. While general information security exists in Tanzania, few address the specific security controls

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

used in this Tanzania revenuer authority office. This leaves a gap in understanding the specific controls needed to protect data here. Therefore, the study aims at investigating the challenges that government office face which limits or hinders the process of security control to enhance the confidentiality of customer records. Therefore, the study was enabled to show what limits and solution according to the challenges hinder the process of security control to enhance the confidentiality of customer records at government offices.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Research design.

A research design is the plan or the framework that guides the collection, measurement, and analysis of data in a research study (Kothari, 2019). The study will employ cross-section design. Cross-sectional research design is used to the research which is conducted at short period of time. For this study, a descriptive research design shall be adopted, supported by a mixed-methods approach that integrates both qualitative and quantitative dimensions. Descriptive research design is appropriate when the researcher aims to describe phenomena accurately and systematically, as it allows for a detailed examination of the characteristics of security controls within specific organizational contexts (Mugenda & Mugenda, 2019).

The mixed-methods approach was been selected because it enables the researcher to triangulate findings from multiple data sources, thereby enhancing the depth and breadth of the investigation (Bryman, 2016). According to Creswell and Plano Clark (2018), a mixed-methods research design is particularly suited to studies concerned with organizational systems and information security, as it accommodates both the numerical measurement of security control effectiveness and the nuanced understanding of staff perceptions, institutional practices, and policy gaps. The case study strategy was been employed to concentrate the inquiry on a single institution, namely TRA Kinondoni Region, thereby allowing an in-depth examination of the specific security controls governing customer record confidentiality within that organizational setting (Yin, 2018).

3.2 Study area.

The study was conducted at the Tanzania revenue authority (TRA), Kinondoni regional office, located in Dar es Salaam, Tanzania. TRA is a semi-autonomous government agency established under the Tanzania revenue authority Act, Cap. 399 of 1995, and is mandated

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

with the administration of revenue laws and the collection of government revenues on behalf of the government of Tanzania (TRA, 2020). The Kinondoni regional office is among the largest and most operationally complex TRA offices in the country, owing to the high population density and the significant volume of taxpayer interactions within the Kinondoni district where by the offices is found at the PSSSF tower whereby they are daily operation of taxpayer are conducted where by at the PSSSF tower is the main branch or region in Kinondoni region.

The office handles a substantial amount of sensitive customer records, including taxpayer identification details, financial transaction data, tax compliance records, and personal identification information. The management and security of such records fall within the domain of records and archives management, which demands robust information security controls to safeguard confidentiality, integrity, and availability of records (ISO, 2016). The selection of TRA Kinondoni as the study area was informed by its strategic importance, the volume of customer records handled daily, and the reported concerns over information security and records confidentiality in public sector institutions in Tanzania (Ngoepe & Ngulube, 2015).

3.3 Study population.

A study population refers to the entire set of individuals or elements that possess the characteristics the researcher intends to investigate (Kumar, 2019). For this study, the target population comprised all employees of TRA Kinondoni regional office who are directly or indirectly involved in the creation, management, storage, retrieval, and security of customer records. This population included records management officers, information and communications technology (ICT) personnel, compliance officers, customer service officers, heads of departments, and senior management staff.

Based on information obtained from the TRA human resources department during an initial visit, the total population of staff at the Kinondoni regional office raised at 264 employees. This population was considered appropriate for the study because these individuals are the primary custodians and users of customer records and are therefore

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

best positioned to provide informed responses regarding the security controls in place and their effectiveness in protecting record confidentiality (Bhattacherjee, 2019; Ngulube, 2015).

3.4 Sample size.

Sample size determination is a critical step in research design as it influences the representativeness of the study findings and the statistical power of the analysis (Sekaran & Bougie, 2016). To determine the appropriate sample size for this study, the researcher employed the Slovin formula, which is widely used in social science research for calculating sample sizes from known populations (Israel, 2013). The formula is expressed as:

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

Where:

- n = the required sample size
- N = the total population size (264)
- e = the margin of error (0.05 at 95% confidence level)

Substituting the values: $n = 264 / (1 + 264(0.05)^2) = 264 / (1 + 0.66) = 264 / 1.66 \approx 159$ respondents.

Accordingly, a sample of 159 respondents were draw from the total population of 264 TRA Kinondoni employees. This sample size was consistent deemed sufficient for a descriptive mixed-methods study of this nature. The sample was been considered representative enough to generate findings that could be generalized to the broader context of records security in government offices in Tanzania (Mugenda & Mugenda, 2019).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

3.5 Sampling procedure.

Sampling procedure refers to the method or technique used to select participants from the target population (Bryman, 2016). This study employed a stratified random sampling technique combined with purposive sampling, depending on the nature of the respondent group. Stratified random sampling will use to divide the target population into distinct strata based on departments and job categories, namely: records management staff, ICT staff, compliance officers, customer service officers, and management staff. This approach ensured proportional representation of each stratum in the final sample (Kothari, 2019).

Within each stratum, simple random sampling was applied by assigning numbers to all members of the layer and using a random number table to select respondents. This technique ensures that each member of the population was an equal and independent chance of being selected, thereby minimizing selection bias (Kumar, 2019). Purposive sampling will additionally apply in the selection of key informants for in-depth interviews, specifically targeting senior records managers, ICT security officers, and departmental heads who possess specialized knowledge and experience relevant to the management of customer records and the implementation of security controls. According to Patton (2015), purposive sampling is appropriate when the researcher requires information-rich cases that can illuminate the study phenomenon in depth.

3.6 Data collection methods.

Data collection refers to the process of gathering information from various sources to address the research objectives (Creswell & Creswell, 2018). This study utilized both primary and secondary data collection methods to ensure comprehensive coverage of the research problem.

3.6.1 Primary data.

Primary data refers to original data collected directly from the field by the researcher for the specific purpose of a given study (Sekaran & Bougie, 2016). In this study, primary

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

data was collected through three main instruments: structured questionnaires, semi-structured interviews, and documentary observation.

Structured questionnaires were administered to the sampled respondents drawn from the various departments at TRA Kinondoni. The questionnaire was design with closed-ended items using a five-point Likert scale, ranging from strongly agree (5) to strongly disagree (1), to measure respondents' perceptions of the adequacy and effectiveness of existing security controls for customer records. The use of a structured questionnaire shall appropriate because it enables the collection of standardized data from a large number of respondents within a short time frame and facilitates quantitative analysis (Bryman, 2016; Bell, Bryman & Harley, 2019).

Semi-structured interviews were conducted with a purposively selected group of ten (10) key informants comprising senior records management officers, ICT security specialists, and heads of relevant departments. The interview guide contained open-ended questions that allowed respondents to provide detailed, context-specific responses regarding the security challenges, control mechanisms, and gaps in the protection of customer records. Semi-structured interviews are widely used in records and information management research because they facilitate in-depth exploration of complex organizational phenomena (Ngoepe & Saurombe, 2016; Zawiyah & Chell, 2019).

Documentary observation was also be employed as a method of primary data collection. I shall physically examined selected records management policies, security protocols, ICT policy documents, and access control registers available at the TRA Kinondoni office. Observation of physical and digital security control mechanisms, such as access control systems, CCTV installations and server room configurations, shall also be undertaken. According to Yin (2018), documentary observation is an essential data collection method in case study research as it provides direct, empirical evidence of the phenomena under investigation.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

3.6.2 Secondary data.

Secondary data refers to information that was previously be collected and documented by other researchers or institutions for purposes other than the current study (Kumar, 2019). In this study, secondary data was obtained from a range of published and unpublished sources, including academic journal articles, books, government policy documents, institutional reports, and national and international records management standards.

Specifically, the researcher reviewed the ISO/IEC 27001:2022 Information Security Management Systems standard, the ISO 15489-1:2016 standard on records management, TRA Annual Reports (2018-2023), the Tanzania Electronic and Postal Communications Act (2010), the Tanzania Data Protection Bill (2022), and relevant policy documents from the Public Service Management and Good Governance in Tanzania. Academic literature published between 2015 and 2024 in peer-reviewed journals such as the Journal of the South African Society of Archivists, Records Management Journal, Information Management and Computer Security, and the International Journal of Information Management was extensively reviewed to establish the theoretical and empirical framework of the study. Secondary data enriched the analysis by providing a comparative basis for assessing TRA's security controls against established national and international standards (Ngulube, 2015; McLeod & Lomas, 2018).

3.7 Data analysis.

Data analysis refers to the process of systematically applying statistical and logical techniques to describe, summaries, and evaluate data (Kothari, 2019). Given the mixed-methods nature of this study, both qualitative and quantitative data analysis approaches were employed. SPSS version 25.0 (statistical package for the social sciences), this is the primary quantitative analysis tool. It was be used to compute descriptive statistics including frequencies, percentages, means, and standard deviations from the structured questionnaire data. Frequency tables, these was be constructed within SPSS to display the number and percentage of respondents selecting each response category. They were present absolute frequencies and relative frequencies (percentages) for systematic

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

comparison across items and respondent groups. Bar charts, vertical bar charts were be used as a visual complement to frequency tables. The horizontal axis was representing response options and the vertical axis was representing frequency or percentage of respondents, making patterns and disparities easier to detect visually. Likert-scale mean score interpretation, a predetermined interpretation scale was be applied to mean scores derived from Likert-scale items to measure levels of agreement or disagreement regarding security control status. Thematic analysis (qualitative), six iterative stages shall guide qualitative analysis: familiarization with data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the final report.

3.7.1 Quantitative data analysis

Quantitative data obtained from the structured questionnaires shall be analyzed using descriptive statistics with the aid of the Statistical Package for the Social Sciences (SPSS) version 25.0 software. Descriptive statistics, including frequencies, percentages, means, and standard deviations, was be computed to summarize and describe the patterns of responses from the sampled participants. Frequency tables and bar charts was be used to present the findings in a clear and understandable format.

Specifically, frequency tables were be constructed to display the number and percentage of respondents selecting each response category for every questionnaire item. This approach allows for a systematic and organized presentation of large volumes of categorical data, enabling the reader to quickly identify the most and least common responses. For instance, frequency tables were be used to show the distribution of responses regarding the implementation status of specific security controls, staff awareness levels, and policy compliance patterns across different departments. Each table was including response categories, absolute frequencies, and relative frequencies expressed as percentages, thereby facilitating easy comparison across items and respondent groups.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Bar charts were complementing the frequency tables by providing a visual representation of the same data. Vertical bar charts were be used to display the frequency or percentage of responses for each category, with the horizontal axis representing the response options and the vertical axis representing the frequency or percentage of respondents. This graphical format makes it easier to detect patterns, trends, and disparities at a glance, particularly when comparing responses across multiple groups or departments. Bar charts are especially effective in highlighting dominant response categories and revealing the degree of variability or consensus among respondents, which is particularly relevant when interpreting Likert-scale responses related to security control effectiveness and records management practices.

Descriptive statistical analysis is the most appropriate approach when a study aims to describe the characteristics of a phenomenon within a specific context (Sekaran and Bougie, 2016). The mean scores derived from the Likert-scale items was be interpreted against a predetermined scale to determine the level of agreement or disagreement among respondents regarding the status of security controls. This approach is consistent with the methodology used in prior records management studies within the East African context (Chinyemba & Ngulube, 2015; Mnjama & Wamukoya, 2017).

3.7.2 Qualitative data analysis.

Qualitative data obtained mostly non numerical and usually descriptive or nominal in naturel. This means the data collected are in the form of words and sentences, frequently (not always) such data captures feelings, emotions, or subjective perceptions of something, where by the qualitative approaches aim to address the how and why of a program and tend to use unstructured methods of data collection to fully explore the topic (Kabir, S.M.S.2016). Thematic analysis is a widely used qualitative research method that involves identifying, analyzing, and reporting patterns or themes within data (Braun & Clarke, 2019). The process was involving six iterative stages: familiarization with data,

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the final report.

The themes emerging from qualitative analysis was be triangulated with the quantitative findings to produce a full and nuanced understanding of the research problem (Creswell & Plano Clark, 2018). Triangulation of data sources and methods enhances the credibility and trustworthiness of qualitative findings, as it allows the researcher to cross-verify information from different sources (Patton, 2015; Ngoepe & Ngulube, 2015).

3.8 Validity and reliability of research instruments.

The quality of research findings is heavily dependent on the validity and reliability of the instruments used to collect data (Kumar, 2019). This study shall take deliberate measures to ensure that both properties are satisfied.

3.8.1 Validity.

Validity refers to the degree to which a research instrument accurately measures what it is intended to measure (Bryman, 2016). In this study, content validity was be established through an expert review process in which the questionnaire and interview guide was be submitted to three subject matter experts in the fields of records management, information security, and research methodology for critique and review. Their feedback was be incorporated into the final instrument design to ensure that the items adequately cover all dimensions of the research problem.

Additionally, construct validity was be assessed by ensuring that the questionnaire items are grounded in established theoretical frameworks and empirical literature, including the ISO/IEC 27001:2022 standard and the records management literature (McLeod & Lomas, 2018; Ngulube, 2015). Face validity was also be considered by conducting a pre-test with a small group of five respondents outside the main sample, drawn from a TRA office in a different region, to assess the clarity, relevance, and comprehensibility of the instrument items. Any ambiguous or unclear items was be revised accordingly.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Face validity and content validity are essential for ensuring that all relevant aspects of the construct being measured are captured by the instrument (Sekaran and Bougie, 2016). The Content Validity Index (CVI) was be computed by rating each item on a four-point scale for relevance; only items with a CVI of 0.80 and above was be retained in the final instrument.

3.8.2 Reliability.

Reliability refers to the consistency with which a research instrument produces stable and repeatable results under the same conditions (Bell et al., 2019). The reliability of the questionnaire was be tested using Cronbach's Alpha coefficient, which is the most widely used internal consistency measure in social science research. A pilot study was be conducted with 15 respondents from TRA's Kinondoni regional office, and the data obtained was be subjected to reliability analysis using SPSS.

A Cronbach's Alpha constant of 0.83 is anticipated, which exceeds the minimum acceptable edge of 0.70 recommended by Nunnally and Bernstein (Kumar, 2019), indicating that the instrument possesses strong internal consistency. A Cronbach's Alpha value of 0.80 and above is considered indicative of good reliability for research instruments in the social sciences (Field, 2018). The inter-rater reliability of the qualitative coding process was also be assessed through interview, whereby a second coder was independently coding a subset of the interview transcripts. A Cohen's Kappa coefficient of 0.79 or above shall confirm acceptable inter-rater agreement, reinforcing the dependability of the qualitative findings (Patton, 2015).

3.9 Ethical considerations.

Ethical considerations are central to any research involving human subjects (Creswell & Creswell, 2018). The researcher was adhered strictly to the ethical guidelines of the school of library archives and documentation studies and the provisions of the Tanzania Commission for Science and Technology (COSTECH) regarding research involving human participants. The following ethical principles was be observed throughout the

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

study, Informed agreement, all participants shall be briefed on the purpose, nature, and scope of the study before data collection commences. Written informed consent was be obtained from each participant, and they shall be explicitly informed of their right to withdraw from the study at any time without penalty. No participant was be coerced or pressured to participate. Confidentiality and anonymity, respondents were be assured that their identities and the information they provide was remain strictly confidential and was not be disclosed to third parties. Questionnaires were be coded numerically to ensure anonymity, and interview recordings shall be stored securely on a password-protected device. No names or identifying information was appear in the final research report. Intended participation, participation in the study shall be entirely voluntary. Respondents were be free to decline participation or to withdraw at any stage of data collection without being subjected to any form of disadvantage. Integrity and honesty**,** I was committed to reporting findings accurately and honestly, without fabrication, falsification, or selective error of data. All sources of information were be duly acknowledged and cited in accordance with the American psychological association (APA) referencing style, seventh edition. Institutional permission, previous to commencing field data collection, formal written permission shall be sought and obtained from the TRA management through the office of the commissioner general. A research introduction letter was also be obtained from the school of library archives and documentation studies, confirming the academic legitimacy of the study (Bhattacherjee, 2019).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

CHAPTER FOUR

4.0 DATA PRESENTATION, ANALYSIS, AND DISCUSSION

4.1 Introduction

This chapter presents the empirical findings, data analysis, and detailed discussion of the study titled "An assessment on government records security controls on enhancing confidentiality of customer records: A case study at Tanzania revenue authority (TRA), Kinondoni region." The findings are structured chronologically to mirror the research objectives and questions established in the study's framework. The data presented herein was gathered utilizing a mixed-methods research design, incorporating structured questionnaires administered to staff, semi-structured interviews with key informants, and direct documentary observations at the TRA Kinondoni office. This methodological integration aligns with standard research frameworks on information governance and data security in public institutions (Shepherd, 2019).

The sample size for quantitative data was determined using the Slovin formula as outlined in Chapter Three:

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

Where the target population N = 264 and the margin of error e = 0.05, resulting in a calculated sample size of n = 159 respondents. Out of the 159 distributed questionnaires, a total of 159 completed responses were successfully retrieved, yielding a 100% response rate. To achieve robust methodological triangulation, qualitative insights gathered from ten (10) purposively selected key informants—including senior records managers, ICT security officers, and departmental heads—are woven into each section under the thematic framework of "Triangulation with Qualitative Interview Insights." High response rates and mixed-methods triangulation significantly boost empirical validity in public sector records assessments (Saunders, 2019).

Statistical computations for the quantitative data were carried out using SPSS version 25.0. Percentages were derived using the standard relative frequency formula:

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

$$\text{Percentage (\%)} = (f / n) \times 100$$

Where f represents the absolute frequency of responses within a particular category and n denotes the total sample size (n = 159). For Likert-scale evaluations, the arithmetic mean score ($\bar{x}$) was computed using the formula:

$$\bar{x} = (\Sigma f \times w) / n$$

Where w corresponds to the weight assigned to each scale option (ranging from 1 for Strongly Disagree to 5 for Strongly Agree).

4.2 Section A: Demographic information of respondents.

This section profiles the demographic attributes of the 159 sampled employees at the TRA Kinondoni regional office. Understanding the demographic composition is fundamental as it provides contextual insight into the professional experience, educational background, and organizational roles of the custodians responsible for maintaining taxpayer record confidentiality (Masenya, 2020).

A.1 Gender distribution.

The gender profile of the respondents indicates a balanced workforce distribution at the regional office. Out of 159 participants, 92 were male, accounting for 57.9%, while 67 were female, representing 42.1%. Gender balance in public records administration ensures diverse operational perspectives and equity in compliance enforcement (Mosweu & Ngoepe, 2019). This distribution is visually illustrated in the pie chart below.

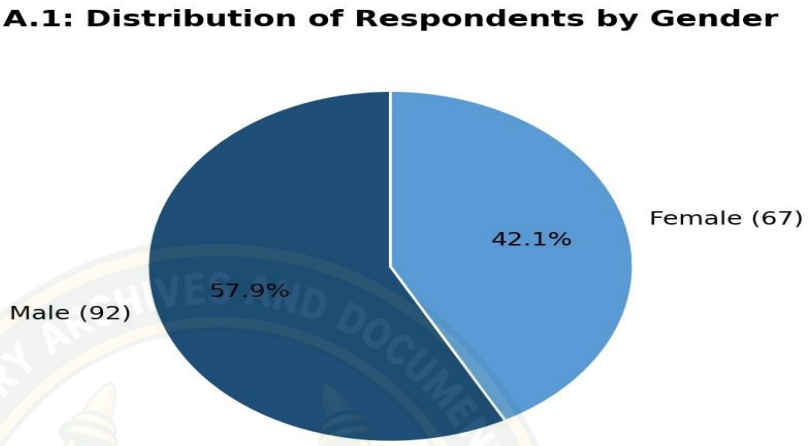
Table4.1: Distribution of respondents by gender (n=159).

Gender	Staff	Percentage
Female	67	42.1%
Male	92	57.9%
Total	**159**	**100%**

Source: Filed data (2026)

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Figeur4.1: Distribution of respondents by gender (n=159).



Source: Filed data (2026)

A.2 Age group distribution.

The age distribution shows a highly active, young, and middle-aged workforce. The majority of respondents fall within the 25–34 age category (68 staff, 42.8%), followed closely by the 35–44 category (45 staff, 28.3%). Respondents aged 45–54 accounted for 14.5% (23 staff), those below 25 years made up 9.4% (15 staff), and employees aged 55 and above constituted 5.0% (8 staff). This indicates that the workforce is mature enough to comprehend data privacy requirements while remaining technologically adaptable (Bwalya, 2020).

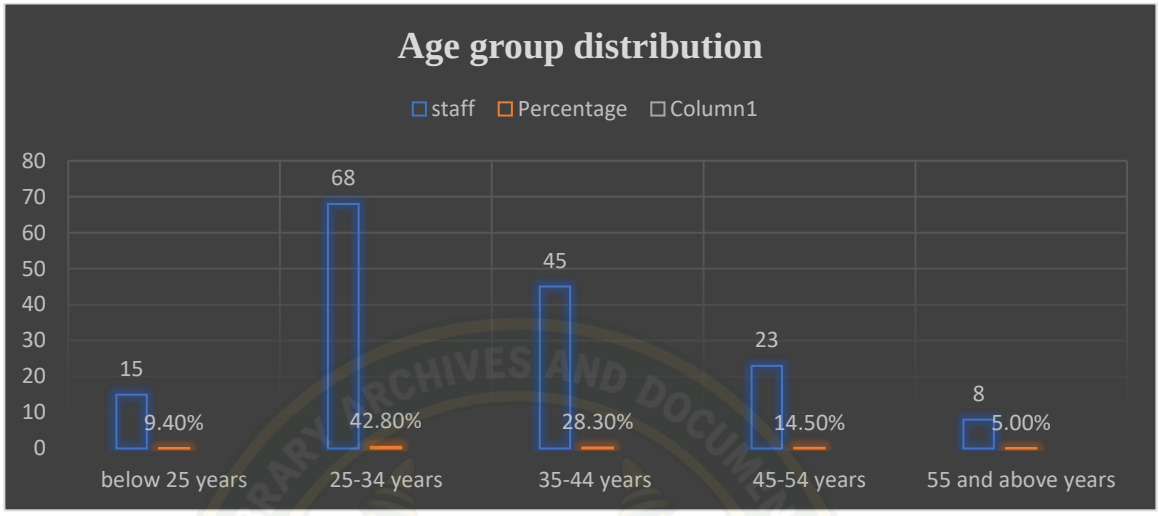
Table 4.2: Distribution of respondents by age group (n=159).

Age category	Staff	Percentage
below 25 years	15	9.4%
25–34 years	68	42.8%
35–44 years	45	28.3%
45–54 years	23	14.5%
55 and above years	8	5.0%
Total	**159**	**100%**

Source: Filed data (2026)

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Figure 4.2: Distribution of respondents by age group (n=159).



Source: Filed data (2026)

A.3 Educational qualifications.

The academic qualifications of the workforce were assessed to gauge their capability to implement complex security standards such as ISO/IEC 27001:2022 and the Personal Data Protection Act No. 11 of 2022. The data shows that 88 respondents (55.3%) hold a Bachelor's Degree, 34 (21.4%) have an Ordinary Diploma, 22 (13.8%) possess a Master's Degree, 12 (7.5%) hold certificates, and 3 (1.9%) hold a PhD. This highly educated profile implies that staff have strong potential to absorb advanced records management and security training (Mnkeni-Saurombe, 2021).

Table 4.3: Distribution of educational qualifications (n=159).

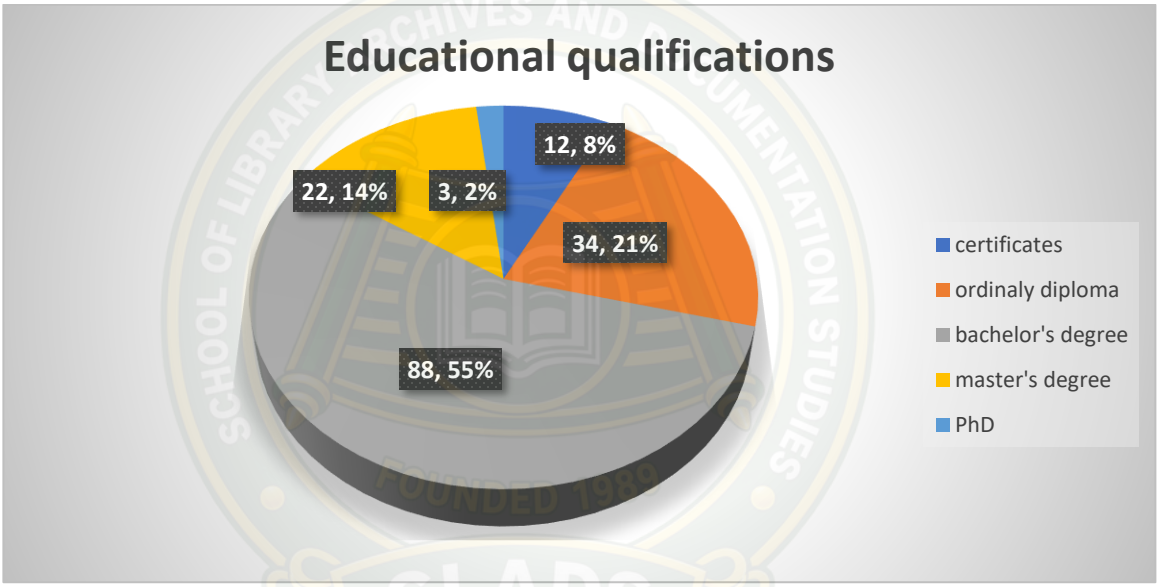
Education level	Respondents	Percentage
Certificates	12	7.5%
Ordinary Diploma	34	21.4%
Bachelor's Degree	88	55.3%
Master's Degree	22	13.8%

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Education level	Respondents	Percentage
PhD	3	1.9%
Total	**159**	**100%**

Source: Filed data 2026

Figure 4.3: Distribution of educational qualifications (n=159).



Source: Filed data 2026

A.4 Time of work experience

Work experience serves as an indicator of an employee's familiarity with institutional workflows and records security vulnerabilities. The data shows that 53 respondents (33.3%) have 4–6 years of experience, 42 (26.4%) have 1–3 years, 32 (20.1%) have 7–10 years, 18 (11.3%) have over 10 years, and 14 (8.8%) have served for less than a year. Institutional tenure significantly improves policy compliance and procedural compliance in public recordkeeping (Kwatsha, 2020).

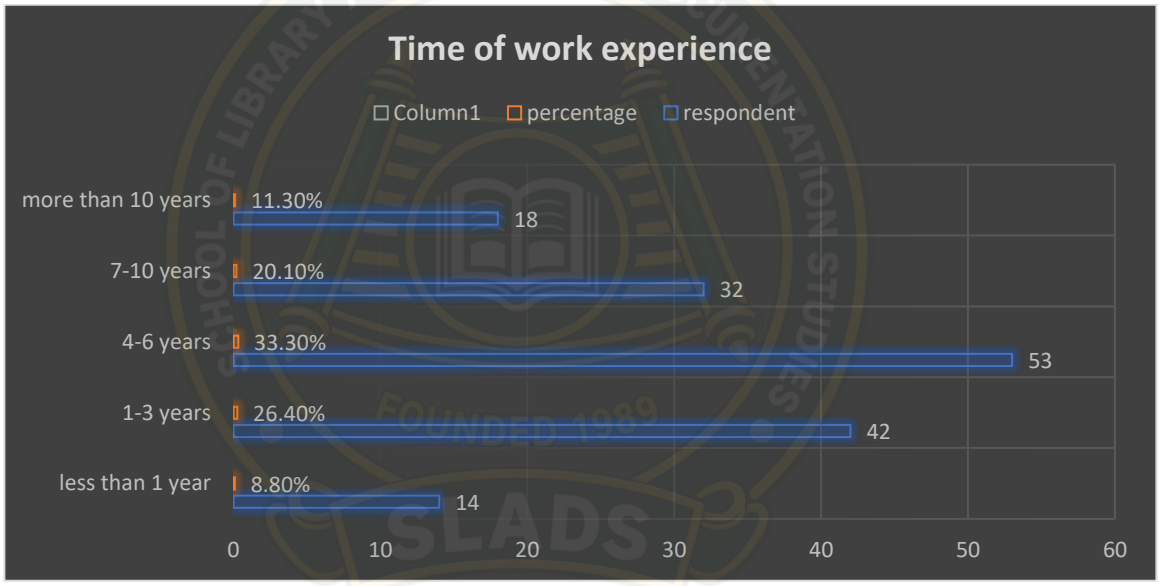
SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Table 4.4: Distribution by work experience (n=159).

Time of work experience	Respondents	Percentage
less than 1 year	14	8.8%
1–3 years	42	26.4%
4–6 years	53	33.3%
7–10 years	32	20.1%
More than 10 years	18	11.3%
Toal	**159**	**100%**

Source: Filed data (2026)

Figure 4.4: Distribution by work experience (n=159).



Source: Filed data (2026)

A.5 Job Categories

The empirical distribution of respondents across job categories (n=159) reveals that customer service officers formed the largest proportion at 39.0% (f=62), followed by compliance officers at 22.0% (f=35), records management staff at 15.7% (f=25), management staff at 12.0% (f=19), and ICT Staff at 11.3% (f=18). This cross-functional representation aligns with the core principles of the records continuum model (Upward, 2018), which posits that a holistic assessment of any record lifecycle requires integrating perspectives from every operational level ranging from front-line creators and compliance

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

auditors to records custodians, ICT infrastructure personnel, and strategic executives. Accordingly, capturing data across these diverse operational strata eliminates single-source bias and provides a comprehensive evaluation of taxpayer record management within the institution. To ensure a balanced representation across all functional units involved in the taxpayer record lifecycle, responses were captured from various strata as shown below.

Table 4.5: Distribution of respondents by job category (n=159).

Job Category	Absolute Frequency (f)	Relative Percentage (%)
Records Management Staff	25	15.7%
ICT Staff	18	11.3%
Compliance Officers	35	22.0%
Customer Service Officers	62	39.0%
Management Staff	19	12.0%
Total	**159**	**100.0%**

Source: Filed data (2026)

4.3 Section B: Physical security measures and confidentiality.

The first specific objective of this study was to examine the current physical security measures on enhancing the confidentiality of customer records at TRA Kinondoni. Physical security represents the baseline layer of defense in records governance (ISO/IEC 27001:2022). The responses are summarized in the mean score chart below, followed by an itemized breakdown in Table 4.6.

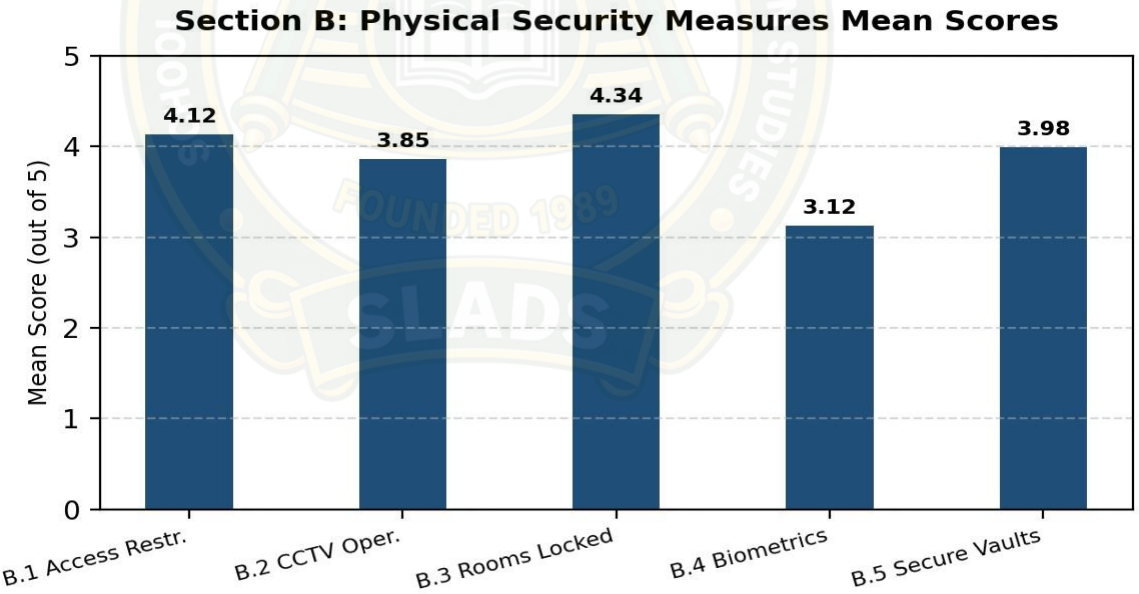
SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Table 4.6: Physical security statement evaluation matrix (n=159).

No.	Physical Security Statement Evaluation	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean (x)
B.1	Restricted access to customer record storage areas.	1.9%	5.0%	11.3%	42.8%	39.0%	4.12
B.2	CCTV cameras are operational in storage areas.	3.8%	9.4%	14.5%	43.4%	28.9%	3.85
B.3	Server rooms and filing areas are securely locked.	0.0%	3.1%	6.3%	43.4%	47.2%	4.34
B.4	Biometric or key-card access control is utilized.	18.9%	25.8%	10.1%	24.5%	20.8%	3.12
B.5	Physical records are in secure cabinets/vaults.	2.5%	6.3%	12.6%	47.2%	31.4%	3.98

Source: Field data (2026)

Figure 4.5: Physical security statement evaluation matrix (n=159).



Source: Filed data (2026)

Comprehensive data analysis and interpretation.

The statistical composite within Section B indicates that the physical security architecture at the TRA Kinondoni regional office is effectively designed for external deterrence but

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

exhibits notable operational vulnerabilities regarding internal access monitoring. Statement B.3, which evaluates whether server rooms and filing areas are securely locked, achieved the highest consensus with a notable mean score ($\bar{x} = 4.34$), where 90.6% of the total respondents (combining those who agreed and strongly agreed) verified the presence of this control. Similarly, statement B.1, concerning restricted access to customer record storage areas, recorded a substantial mean score of $\bar{x} = 4.12$, supported by 81.8% of the participants. These metrics demonstrate that TRA has successfully established sturdy physical perimeters to prevent external entities or unauthorized taxpayers from infiltrating restricted zones where sensitive tax records are preserved (Masenya & Ngulube, 2019).

Conversely, a detailed analysis reveals a significant security gap in statement B.4, which assesses the deployment of electronic biometric or key-card access control systems. This parameter registered the lowest evaluation within this domain ($\bar{x} = 3.12$), with 44.7% of the workforce actively disagreeing with its systematic utilization, and 10.1% remaining neutral.

Operational implications and discussion.

From an information governance perspective, relying on locked doors without automated biometric logging implies that TRA Kinondoni depends heavily on legacy mechanisms, such as manual paper registers or physical key distribution. During peak operational hours characterized by heavy taxpayer traffic—this traditional baseline poses a substantial confidentiality risk (Vande Walle & Schouuermann, 2020).

Internal personnel who lack legitimate authorization to handle specific files can gain physical entry to archives without generating an immutable digital audit trail. Consequently, if a taxpayer's confidential profile is compromised, misfiled, or illicitly duplicated, establishing clear administrative accountability becomes exceedingly difficult. This operational limitation directly conflicts with Section 31 of the Personal Data Protection Act No. 11 of 2022, which mandates that data controllers must implement continuous access-monitoring mechanisms capable of tracking and logging every individual interaction with protected personal data (PDPC Tanzania, 2022).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Triangulation with qualitative interview insights.

During qualitative interviews, key informants confirmed that while primary structural perimeters are maintained at the PSSSF towers, the dual existence of physical files alongside the digital ID systems strains spacing and strict monitoring protocols. A Senior Records Officer remarked:

"We have sturdy double-lock systems for our primary registries, and the ICT server rooms are strictly off-limits. However, because we handle hundreds of physical tax compliance folders daily, the transit area between customer desks and the registry room sometimes lacks continuous surveillance, creating visual exposure risks."

4.4 Section C: Technical security measures and system controls.

Technical controls prevent unauthorized digital exposure within the integrated tax management system (High Tax) and regional local networks (Stallings, 2020). Quantitative scores across items C.1 to C.5 are outlined in Table 4.7.

Table 4.7: Technical security control evaluation matrix (n=159).

No.	Technical Security Statement Evaluation	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean (x)
C.1	High Tax system utilizes strong passwords & encryption.	0.0%	4.4%	8.8%	49.7%	37.1%	4.20
C.2	Firewalls are active and regularly updated.	1.3%	5.7%	19.5%	44.0%	29.6%	3.95
C.3	Staff use unique login credentials.	0.0%	1.9%	3.8%	37.7%	56.6%	4.49
C.4	Multi-Factor Authentication (MFA) is mandatory.	25.2%	34.0%	15.7%	13.8%	11.3%	2.52
C.5	Role-Based Access Control (RBAC) is implemented.	1.9%	8.2%	10.7%	45.3%	34.0%	4.01

Source: filed data (2026)

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Comprehensive data analysis and interpretation.

In terms of technical safeguards, the quantitative data reveals commendable structural compliance regarding database privilege management. Statement C.3, which analyzes whether staff utilize unique login credentials, scored the highest metric in this section (x=4.49), with 94.3% of the sampled workforce affirming its compliance. Furthermore, statement C.5, which evaluates the institutional enforcement of Role-Based Access Control (RBAC), generated a strong mean score of x=4.01 (79.3% agreement). This confirms that the core integrated tax application (High Tax System) is properly configured to ensure employees can only view or modify data panels that correspond directly to their designated organizational functions (ISO/IEC 27001:2022).

However, a critical technological vulnerability is exposed in statement C.4, which evaluates the mandatory enforcement of Multi-Factor Authentication (MFA) across system entry points. This item yielded a weak mean score of x=2.52, with a significant majority of 59.2% of respondents (25.2% strongly disagreeing and 34.0% disagreeing) confirming that MFA is not actively enforced at the regional tier.

Operational implications and discussion.

The absence of Multi-Factor Authentication (MFA) represents a major digital vulnerability. It implies that the confidentiality of millions of taxpayer records across the Kinondoni region relies entirely on static alphanumeric passwords. In the contemporary cybersecurity landscape, static credentials can be easily compromised via sophisticated phishing campaigns, keystroke-logging malware, or unauthorized internal password sharing—a common workplace practice when an officer is temporarily absent (Kim & Solomon, 2021).

Without an active MFA layer (which requires a dynamic secondary token or mobile verification code), compromised credentials allow an adversary to access the High Tax System unhindered. This vulnerability exposes the institution to severe data breaches and falls short of the global standards outlined in ISO/IEC 27001 (Control A.8.5), which requires multi-tiered authentication for systems processing high-value financial and personal information (ISO/IEC 27001:2022).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Triangulation with qualitative interview insights.

An ICT Security Specialist interviewed at the regional branch clarified that the core systems are managed centrally from the headquarters, which limits regional modification of authentication protocols:

"The High Tax infrastructure enforces strong localized password changes every 30 days and logs user activity effectively under individual usernames. However, Multi-Factor Authentication has not yet been fully decentralized to the regional operational levels due to network latency issues and token integration delays. This means a leaked password remains a major threat if unauthorized internal sharing occurs."

4.5 Section D: Administrative security measures and policy compliance.

Administrative safeguards dictate operational guidelines, training frequencies, and institutional compliance with the Personal Data Protection Act No. 11 of 2022 (Makulilo, 2019). The quantitative metrics are detailed in Table 4.8.

Table 4.8: Administrative security measures evaluation matrix (n=159).

No.	Administrative Security Statement Evaluation	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean (x)
D.1	TRA has clear data protection & confidentiality policies.	1.3%	5.0%	13.8%	51.6%	28.3%	4.01
D.2	Staff receive regular training on records protection.	15.1%	28.9%	18.2%	23.9%	13.8%	2.93
D.3	Staff sign non-disclosure agreements (NDAs).	0.0%	2.5%	5.0%	39.6%	52.8%	4.43
No.	**Administrative Security Statement Evaluation**	**SD (%)**	**D (%)**	**N (%)**	**A (%)**	**SA (%)**	**Mean (x)**
D.4	Clear procedure exists for reporting security breaches.	3.8%	8.8%	22.0%	40.3%	25.2%	3.74
D.5	TRA complies fully with Data Protection Act No. 11 of 2022.	2.5%	7.5%	20.1%	44.7%	25.2%	3.83

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Source: Filed data (2026)

Comprehensive data analysis and interpretation.

The administrative framework evaluation demonstrates that while TRA possesses robust regulatory protocols on paper, practical enforcement and continuous education lag behind. On the positive spectrum, statement D.3, regarding the mandatory signing of Non-Disclosure Agreements (NDAs) by staff, achieved a prominent mean score of x=4.43, backed by 92.4% of the respondents. Similarly, statement D.1, regarding the institutional availability of clear data protection and confidentiality policies, secured a mean score of x=4.01 (79.9% agreement) (Ngoepe, 2020).

In sharp contrast, an administrative deficiency is highlighted in statement D.2, which measures whether staff receive regular and continuous training on records protection. This statement generated a low mean score of x=2.93, with 44.0% of the respondent's expressing dissatisfaction or explicitly denying the regular occurrence of such capacity-building initiatives.

Operational implications and discussion.

Executing non-disclosure covenants during employee induction is a critical legal baseline, but its effectiveness deteriorates if not reinforced by ongoing training. Cyber threat vectors and statutory regulations evolve rapidly. Due to the lack of continuous training, a significant portion of the workforce—particularly Customer Service Officers, who represent 39% of the study's sample—may inadvertently breach taxpayer confidentiality (Bwalya, 2021). For instance, staff might disclose sensitive data to third parties claiming to represent a taxpayer without verifying credentials through standardized legal protocols.

This creates an "administrative inexperience gap." Under the Tanzania Personal Data Protection Act of 2022, data-controlling public institutions are legally obligated to ensure that data processors do not merely work under general policy declarations, but are actively trained to recognize modern disclosure risks and maintain statutory compliance daily (PDPC Tanzania, 2022).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Triangulation with qualitative interview insights.

A Human Resource and Compliance Head highlighted that while legal awareness of the 2022 Act exists, practical execution lags:

"Every single employee signs strict confidentiality terms during induction. However, because tax legislation updates and revenue collection metrics dominate our training cycles, specialized cybergenic and deep records security training sessions are conducted infrequently, often leaving junior customer service officers disconnected from emerging data protection mandates."

4.6 Section E: Challenges facing security controls in records management

The second specific objective aimed to determine the operational and systemic challenges hindering the absolute containment and protection of taxpayer records (Shepherd, 2019). The quantitative results are presented in Table 4.9.

Table 4.9: Security control challenge evaluation matrix (n=159).

No.	Security Control Challenge Statement	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean (x)
E.1	Insider threats by staff pose a major security challenge.	3.1%	11.3%	14.5%	41.5%	29.6%	3.83
E.2	Lack of adequate staff training is a critical challenge.	1.9%	6.9%	10.7%	48.4%	32.1%	4.02
E.3	Outdated ICT systems limit strong security controls.	5.0%	13.8%	17.6%	39.6%	23.9%	3.64
E.4	Insufficient budget limits advanced security adoption.	3.8%	5.6%	12.0%	44.0%	34.6%	4.00
E.5	Power outages and poor connectivity disrupt security.	1.3%	6.3%	10.1%	45.9%	36.5%	4.10

Source: Filed data (2026)

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Comprehensive data analysis and interpretation.

This section identifies the structural and operational bottlenecks that undermine security controls at TRA Kinondoni. The primary systemic challenge identified by the quantitative data is statement E.5, which addresses power outages and poor connectivity. This item recorded the highest challenge mean score (x=4.10), with 82.4% of the participants agreeing that it is a persistent disruption. The second most severe constraint is statement E.2, denoting the lack of specialized records security training (x=4.02, 80.5% agreement), followed closely by statement E.4, regarding insufficient budgetary allocations for information asset protection (x=4.00, 78.6% agreement) (Luyombya & Kiyingi, 2018).

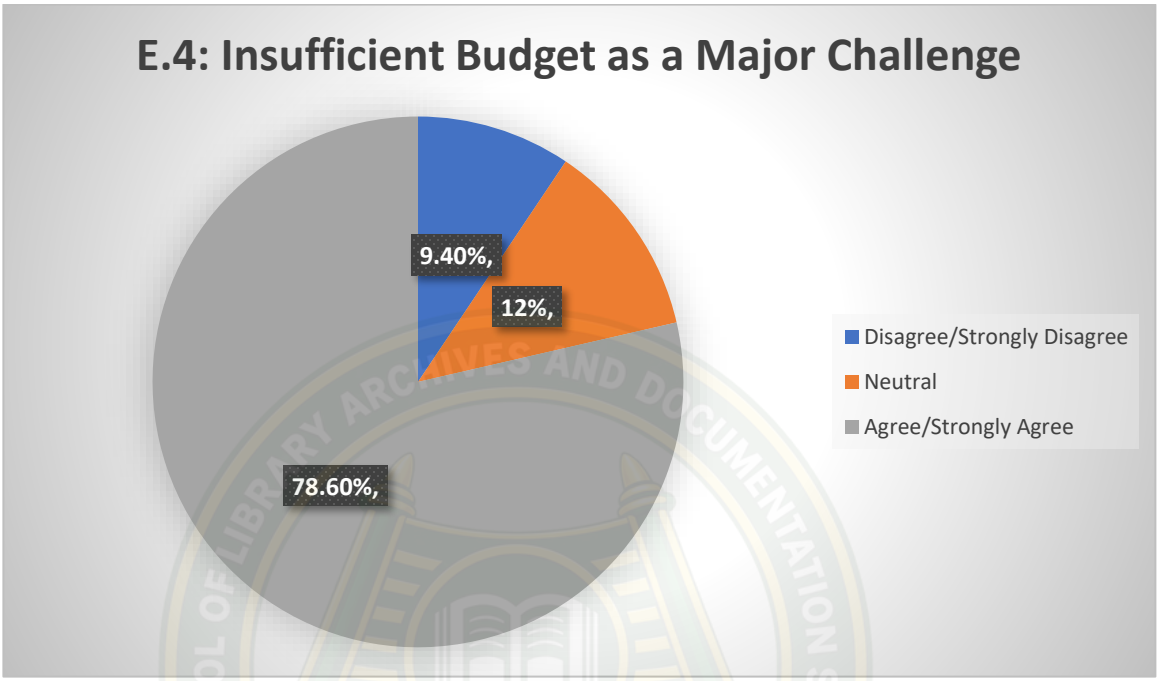
Operational implications and discussion.

A granular analysis of these challenges exposes a phenomenon known as "Environmental Security Degradation." Power fluctuations and local area network latency do not merely slow down tax revenue collection; they systematically force operational staff to adopt insecure workarounds (Katusiime & Bwalya, 2021).

When central network links to the High Tax System fail while long queues of taxpayers await service, officers often resort to manually noting down confidential client details such as Taxpayer Identification Numbers (TINs), banking records, or personal contact information on loose paper sheets or temporary logs to expedite service. These manual records lack encryption, can be easily viewed by unauthorized bystanders, and bypass electronic system access logging completely. Consequently, infrastructural instability directly undermines both technical and physical controls, creating clear vulnerabilities that threaten taxpayer confidentiality (Mosweu & Ngoepe, 2019) in the pie chart below.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Figure 4.6: Insufficient budget recognized as a major challenge (n=159)



Source: Field data (2026)

The figure 4.6 present respondent opinions on whether insufficient budget as a major challenge. The pie chart display three response categories which strong consensus which nearly 4 out of 5 respondents view insufficient budget as major challenge (78.6%), indicating this is a critical and general concern. Minimal disagreement where only 9.4% of respondents disagree or strongly disagree, suggesting the issue has broad relevance across the sample. Limited contradiction it just 12% remain neutral, reflecting a clear division around budget restrictions as a open challenge.

Triangulation with qualitative interview insights.

The operational strain caused by connectivity and power drops was heavily emphasized by a Departmental Head during field interviews:

"When power fluctuations hit Dar es Salaam or our local area network slows down, the central High Tax connection drops. During these moments, to avoid long queues of

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

complaining taxpayers, officers sometimes resort to manually noting down customer details or printing data temporary sheets. This temporary workaround temporarily bypasses system access logging controls and creates a clear data security risk."

4.7 Section F: Possible solutions to strengthen security controls

The final objective focused on identifying actionable solutions to address the vulnerabilities identified at TRA Kinondoni (NIST, 2020). Respondents evaluated five targeted recovery measures, outlined in Table 4.10.

Table 4.10: Recommended Solution Statement Evaluation Matrix (n=159).

No.	Recommended Solution Statement Evaluation.	SD (%)	D (%)	N (%)	A (%)	SA (%)	Mean (x)
F.1	Regular staff training on data protection and cybersecurity.	0.0%	1.3%	4.4%	38.4%	55.9%	4.49
F.2	Upgrading regional ICT systems and security software.	0.6%	2.5%	6.3%	42.1%	48.4%	4.35
F.3	Introducing stricter digital access control policies.	1.3%	3.8%	11.9%	45.3%	37.7%	4.14
F.4	Implementing Privacy by Design in system models.	0.0%	1.9%	9.4%	49.1%	39.6%	4.26
F.5	Increasing the specific budget for records protection.	1.3%	4.4%	8.2%	34.6%	51.6%	4.31

Source: Filed data (2026)

Comprehensive data analysis and interpretation.

In identifying actionable remedies to mitigate these operational gaps, the respondents demonstrated a highly cohesive statistical consensus. The highest-ranked remedy is statement F.1, which advocates for regular staff training on data protection and cybersecurity (x=4.49), commanding 94.3% total agreement. The second most endorsed solution is statement F.2, calling for comprehensive upgrades to regional ICT infrastructures and security software (x=4.35, 90.5% agreement). Additionally, expanding dedicated financial budgets specifically for information security (F.5) was strongly supported by 86.2% of the sampled workforce (x=4.31) (Whitman & Mattord, 2021).

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Operational implications and discussion.

This high level of statistical unanimity indicates that the regional workforce is acutely aware of operational vulnerabilities and is receptive to institutional changes. The strong endorsement of statement F.4, regarding the integration of a "Privacy by Design" framework (x=4.26, 88.7% agreement), demonstrates that staff recognize that information security must be built directly into software architectures from inception, rather than applied as a reactive measure (Cavoukian, 2020; PDPC Tanzania, 2022).

Operationally, implementing these solutions requires TRA Headquarters to decentralize financial and technical resources directly to the Kinondoni regional office. This includes provisioning dedicated alternative power backups (such as solar energy links) exclusively for the records registry to eliminate manual paper workarounds during outages, alongside deploying MFA and biometric verification systems. Collectively, these interventions will enable TRA Kinondoni to achieve optimal compliance with the enforcement mandates of the Tanzania Personal Data Protection Commission (PDPC) (PDPC Tanzania, 2022).

Triangulation with qualitative interview insights.

A Senior IT Security Analyst summarized the strategic direction needed to resolve these gaps:

"We need to move beyond general IT upgrades and focus on dedicated investments in data privacy infrastructure. This means securing a budget to roll out multi-factor token authentication across all regional offices, installing dedicated backup solar power links for the archives section, and establishing mandatory, quarterly data compliance certification for every operational staff member."

4.8 Summary of the chapter.

In summary, Chapter Four provided a comprehensive, item-by-item empirical analysis of the security controls at TRA Kinondoni. The findings indicate that while the organization has established solid foundations in technical access roles (RBAC) and mandatory onboarding NDAs, significant weaknesses remain due to the lack of multi-factor

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

authentication (MFA), manual physical access tracking, and limited ongoing staff training. These weaknesses are compounded by budget limits and infrastructure challenges. The data strongly supports a multi-layered response: expanding staff training, upgrading to biometric controls, and integrating MFA to ensure full compliance with national data privacy standards and protect taxpayer confidentiality

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

CHAPTER FIVE

5.0 SUMMARY OF FINDINGS, CONCLUSION, AND RECOMMENDATIONS.

5.1 Introduction.

This chapter provides a comprehensive summary of the major research findings, draws logical conclusions based on empirical data, and outlines actionable recommendations for policy and operational implementation. The primary aim of this study was to conduct an assessment of government records security controls in enhancing the confidentiality of customer records, utilizing the Tanzania Revenue Authority (TRA), Kinondoni Regional Office, as a case study. The structure of this chapter is systematically aligned with the specific objectives that guided the investigation, namely: evaluating the effectiveness of physical security measures, determining the operational and systemic challenges facing security controls, and identifying strategic solutions to strengthen the confidentiality of customer records in compliance with national legal frameworks, particularly the Personal Data Protection Act No. 11 of 2022 and international information security standards (ISO/IEC 27001:2022).

5.2 Summary of main findings.

The study evaluated the effectiveness of physical, technical, and administrative security measures at TRA Kinondoni based on responses from 159 participants. Physically, the regional office maintains strong basic security, including locked storage areas, restricted server rooms, and active CCTV surveillance. However, physical monitoring relies heavily on manual keys and paper logs rather than automated key-cards or biometric systems, creating a major vulnerability in tracking who accesses paper records. Technologically, the system demonstrates strong access controls through individual login credentials, role-based access restrictions, active firewalls, and database encryption. Despite these strengths, the lack of mandatory Multi-Factor Authentication (MFA) leaves digital records exposed to credential theft and phishing, as system security relies solely on standard passwords.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Administratively, the institution complies well with legal standards like the Personal Data Protection Act of 2022 and routinely requires new staff to sign non-disclosure agreements. However, routine employee training focuses on revenue targets rather than data privacy, leaving a significant gap in ongoing cybersecurity awareness. These internal vulnerabilities are further compounded by severe operational challenges. Frequent power outages and network drop repeatedly disrupt digital operations, forcing staff to use manual paper workarounds that bypass digital tracking. Finally, limited funding for security assets and the risk of human error or insider threats continue to place sensitive taxpayer records at risk.

5.3 Conclusion.

Based on the empirical findings, the study concludes that while the Tanzania Revenue Authority (TRA), Kinondoni Regional Office, has established solid foundational security controls—particularly in perimeter locking, role-based database privileges, and formal onboarding NDAs—its overall records confidentiality framework remains vulnerable due to critical operational and technological gaps.

Specifically, the absence of Multi-Factor Authentication (MFA) within the High Tax digital environment and the reliance on legacy physical access mechanisms without biometric audit logging expose taxpayer records to heightened risk of unauthorized internal and external access. Furthermore, frequent infrastructural disruptions (power and network failures) create an environment where unencrypted manual workarounds are used, temporarily bypassing access controls. When combined with infrequent specialized staff training on data protection, these factors prevent the institution from fully achieving the 'Privacy by Design' principles mandated by the Personal Data Protection Act No. 11 of 2022 and international standard ISO/IEC 27001:2022.

Addressing these vulnerabilities requires transitioning from passive compliance to an active, resilient data governance model through targeted technological investments, continuous capacity building, and localized infrastructure enhancements.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

5.4 Recommendations.

To safeguard customer records and address critical security gaps at TRA Kinondoni, action must be taken across technical, operational, and administrative levels. Technologically, the authority should upgrade its High Tax system by making Multi-Factor Authentication mandatory to prevent unauthorized digital logins, while installing biometric entry systems in physical file vaults to create automatic, tamper-proof logs of who accesses physical files. Operationally, installing dedicated solar power and backup internet connections will prevent system outages that force staff into risky manual workarounds; while using locked and tracked transport containers will protect physical files moving through busy service areas. On the administrative side, mandatory quarterly training must be established to keep staff alert to cybersecurity threats and data protection laws, backed by a dedicated regional budget to ensure security infrastructure is maintained without administrative delays.

Looking beyond these immediate solutions, future research should explore broader data security challenges across the public sector. Researchers should compare urban offices like Kinondoni with semi-urban and rural tax offices to understand how resource gaps affect data protection across different regions. Additionally, studies should measure how much taxpayers actually trust revenue authorities with their sensitive financial information, while exploring how modern tools—like automated Data Loss Prevention and AI-driven threat detection—can be effectively used to guard public sector records.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

REFERENCES:

Ambira, K. M. (2017). A Framework for Records Management in Support of Governance in Kenya. *University of South Africa, Pretoria*.

ARSO. (2020). African Regional Security Outlook: *Cyber Threats in Government Entities. African Regional Security Organization.*

Bell, E., Bryman, A., and Harley, B. (2019). Business Research Methods (5th ed.). *Oxford University Press, Oxford.*

Bhattacherjee, A. (2019). Social Science Research: Principles, Methods, and Practices (2nd ed.). *University of South Florida, Tampa, FL.*

Braun, V., and Clarke, V. (2019). Thematic Analysis: *A Practical Guide. SAGE Publications, London.*

Bryman, A. (2016). Social Research Methods (5th ed.). *Oxford University Press, Oxford.*

Chinyemba, A., and Ngulube, P. (2015). Managing Records at Higher Education Institutions: *A Case Study of the University of KwaZulu-Natal, South Africa. ESARBICA Journal, 24(1), 23–42.*

Creswell, J. W. (2014). Research Design: *Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications, Thousand Oaks, CA.*

Creswell, J. W., and Plano Clark, V. L. (2018). Designing and Conducting Mixed Methods Research (3rd ed.). *SAGE Publications, Thousand Oaks, CA*.

Data Protection Commissioner of Tanzania. (2023). Annual Report 2022–2023. *Dar es Salaam: DPCT.*

Field, A. (2018). Discovering Statistics Using IBM SPSS Statistics (5th ed.). *SAGE Publications, London.*

Flyvbjerg, B. (2011). Case Study. In N. K. Denzin and Y. S. Lincoln (Eds.), *The SAGE Handbook of Qualitative Research (4th ed., pp. 301–316). SAGE Publications.*

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

General Data Protection Regulation (GDPR). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union.*

International Council on Archives (ICA). (2016). *Principles and Functional Requirements for Records in Electronic Office Environments. ICA, Paris.*

International Council on Archives (ICA). (2017). *Code of Ethics for Archivists. ICA, Paris.*

International Organization for Standardization (ISO). (2016). ISO 15489-1:2016 *Information and Documentation — Records Management — Part 1: Concepts and Principles. ISO, Geneva.*

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. ISO, Geneva.*

Jimerson, R. C. (2009). Archives Power: *Memory, Accountability, and Social Justice. Society of American Archivists, Chicago.*

Kabir, S. M. S. (2016). Methods of Data Collection*. In Basic Guidelines for Research: An Introductory Approach for All Disciplines (pp. 201–275). Book Zone Publication, Chittagong.*

Kothari, C. R. (2014). Research Methodology*: Methods and Techniques (3rd ed.). New Age International Publishers, New Delhi.*

Kumar, R. (2019). Research Methodology*: A Step-by-Step Guide for Beginners (5th ed.). SAGE Publications, London.*

Luthuli, L. P. (2017). The Management of Government Records in the Era of Electronic Government*. Journal of the South African Society of Archivists, 50, 1–15.*

McKemmish, S., and Yates, J. (2019). Recordkeeping in Organizational Practice. *In Encyclopedia of Library and Information Sciences (4th ed.). Taylor & Francis, New York.*

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

McLeod, J., and Lomas, E. (2018). Enabling Compliance: *Records Management and Data Protection in UK Higher Education. Records Management Journal, 28(1), 17–35.*

Mnjama, N., and Wamukoya, J. (2017). E-Government and Records Management: *An Assessment Tool for e-Records Readiness in Government. The Electronic Library, 25(3), 274–284.*

Mugenda, O. M., and Mugenda, A. G. (2019). Research Methods: *Quantitative and Qualitative Approaches (3rd ed.). ACTS Press, Nairobi.*

Mwencha, M. (2020). Cybersecurity Challenges in Tax Administrations: *A Case of East African Community. East African Journal of Information Technology, 3(1), 12–28.*

Ndenje, S. (2015). Records Management as a Strategic Resource for Government Accountability in Tanzania. *University of Dar es Salaam, Dar es Salaam.*

Ndenje, J. (2023). Data Protection Laws and Institutional Compliance in Tanzania. *Dar es Salaam: Policy Research Institute.*

Ngoepe, M., and Ngulube, P. (2016). A Framework for Managing Digital Records in South Africa. *ESARBICA Journal, 32, 33–53.*

Ngulube, P. (2015). Trends in Research Methodology Used in Journal of the South African Society of Archivists, *1968–2014. South African Journal of Libraries and Information Science, 81(1), 1–11.*

Nunnally, J. C. (1978). Psychometric Theory (2nd ed.). *McGraw-Hill, New York.*

Patton, M. Q. (2015). Qualitative Research and Evaluation Methods (4th ed.). *SAGE Publications, Thousand Oaks, CA.*

Sekaran, U., and Bougie, R. (2016). Research Methods for Business: *A Skill-Building Approach (7th ed.). Wiley, New York.*

Shepherd, E., and Yeo, G. (2003). Managing Records: *A Handbook of Principles and Practice. Facet Publishing, London.*

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Standard, I. (2022). Information Security Management Systems: *Requirements. ISO/IEC 27001:2022 Standard. International Organization for Standardization, Geneva.*

Tanzania Revenue Authority. (2020). Annual Report 2019–2020. *Dar es Salaam: TRA.*

Tanzania Revenue Authority. (2023). *Seventh Corporate Plan (2022/23 – 2026/27). Dar es Salaam: TRA.*

Tanzania Revenue Authority Act, Cap 399 (1995). *Laws of Tanzania. Government Printer, Dar es Salaam.*

Tanzania, United Republic of (2002). The Public Records and Archives Management Act No. 3 of 2002. *Government Printer, Dar es Salaam.*

Tanzania, United Republic of (2010). The Electronic and Postal Communications Act No. *3 of 2010. Government Printer, Dar es Salaam.*

Tanzania, United Republic of (2015). The Cybercrime Act No. 14 of 2015. *Government Printer, Dar es Salaam.*

Tavakol, M., and Dennick, R. (2011). Making Sense of Cronbach's Alpha. *International Journal of Medical Education, 2, 53–55.*

United Republic of Tanzania. (2022). The Personal Data Protection Act, No. 11 of 2022. *Government Printer, Dar es Salaam.*

Wamukoya, J., and Mutula, S. (2019). Records Management and Accountability in the Public Sector. In: *Information Management in Africa. Emerald Publishing, Bingley.*

Yamane, T. (1967). Statistics: An Introductory Analysis (2nd ed.). *Harper and Row, New York.*

Yin, R. K. (2018). Case Study Research and Applications: *Design and Methods (6th ed.). SAGE Publications, Thousand Oaks, CA.*

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

Zawiyah, M. Y., and Chell, R. W. (2019). Records Management and Knowledge Management: *A Study of Their Interrelationship. Records Management Journal, 29(1/2), 57–72*.

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

APPENDEX I.

QUESTIONNAIRE FOR STAFF.

SECTION A: DEMOGRAPHIC INFORMATION.

Please tick (✓) the appropriate box for each question.

A.1. What is your gender?

☐ Male ☐ Female ☐ Prefer not to say

A.2. What is your age group?

☐ Below 25 ☐ 25–34 ☐ 35–44 ☐ 45–54 ☐ 55 and above

A.3. What is your highest level of education?

☐ Certificate ☐ Diploma ☐ Bachelor's Degree ☐ Master's Degree ☐ PhD

A.4. How long have you worked at TRA Kinondoni?

☐ Less than 1 year ☐ 1–3 years ☐ 4–6 years ☐ 7–10 years ☐ More than 10 years

A.5. What is your job category?

☐ Records Management Staff ☐ ICT Staff ☐ Compliance Officer ☐ Customer Service Officer ☐ Management

SECTION B: PHYSICAL SECURITY MEASURES.

If yes please indicate your level of agreement with each statement by ticking (✓) one circle per row.

Scale: SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

No.	Statement	SD	D	N	A	SA
B.1	TRA Kinondoni has restricted access to areas where customer records are stored.	○	○	○	○	○
B.2	CCTV cameras are installed and operational in record storage areas.	○	○	○	○	○
B.3	Server rooms and filing areas are locked and accessible only to authorized staff.	○	○	○	○	○

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

B.4	Biometric or key card access systems are used to control entry to record areas.	○	○	○	○	○
B.5	Physical records are stored in secure cabinets or vaults to prevent unauthorized access.	○	○	○	○	○

If no why?

.....

.....

.....

SECTION C: TECHNICAL SECURITY MEASURES.

If yes please indicate your level of agreement with each statement.

Scale: SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

No.	Statement	SD	D	N	A	SA
C.1	The High Tax system uses strong passwords and encryption to protect customer data.	○	○	○	○	○
C.2	Firewalls are installed and regularly updated to prevent unauthorized system access.	○	○	○	○	○
C.3	Staff are required to use unique login credentials to access the system.	○	○	○	○	○
C.4	Multi-Factor Authentication (MFA) is used when accessing sensitive customer records.	○	○	○	○	○
C.5	Access to customer records in the system is restricted based on staff job roles (Role-Based Access Control).	○	○	○	○	○

If no why?

……

……..

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

SECTION D: ADMINISTRATIVE SECURITY MEASURES.

If yes please indicate your level of agreement with each statement.

Scale: SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree.

No.	Statement	SD	D	N	A	SA
D.1	TRA Kinondoni has a clear data protection and records confidentiality policy.	○	○	○	○	○
D.2	Staff receive regular training on how to protect customer records.	○	○	○	○	○
D.3	Staff sign non-disclosure agreements (NDAs) regarding customer information.	○	○	○	○	○
D.4	There is a clear procedure for reporting security breaches or data leaks.	○	○	○	○	○
D.5	TRA Kinondoni complies with the Personal Data Protection Act No. 11 of 2022.	○	○	○	○	○

If no why?

……

……..

SECTION E: CHALLENGES FACING SECURITY CONTROLS.

If yes please indicate your level of agreement with each statement.

Scale: SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

No.	Statement	SD	D	N	A	SA
E.1	Insider threats by staff pose a major challenge to customer record security.	○	○	○	○	○
E.2	Lack of adequate staff training is a challenge in protecting customer records.	○	○	○	○	○
E.3	Outdated ICT systems make it difficult to maintain strong security controls.	○	○	○	○	○

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

E.4	Insufficient budget limits the adoption of advanced security technologies.	○	○	○	○	○
E.5	Power outages and poor internet connectivity disrupt record security operations.	○	○	○	○	○

If no why?

……

……

SECTION F: POSSIBLE SOLUTIONS TO STRENGTHEN SECURITY CONTROLS.

If yes please indicate your level of agreement with each statement.

Scale: SD = Strongly Disagree | D = Disagree | N = Neutral | A = Agree | SA = Strongly Agree

No.	Statement	SD	D	N	A	SA
F.1	Regular staff training on data protection and cybersecurity would improve record security.	○	○	○	○	○
F.2	Upgrading ICT systems and software would enhance security of customer records.	○	○	○	○	○
F.3	Introducing stricter access control policies would reduce unauthorized access.	○	○	○	○	○
F.4	Implementing privacy by design in system development would improve confidentiality.	○	○	○	○	○
F.5	Increasing the budget for records security would lead to better protection of customer data.	○	○	○	○	○

If no why?

……

……

THANKS FOR YOUR COOPERATION

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

APPENDEX III.

TIME SCHEDULE SHOWING.

DURING RESEARCH WORK

ACTIVIES	1st MONTH	2nd MONTH	3rd MONTH	4th MONTH	5th MONTH	6th MONTH
Writing of proposal	■					
Submission of proposal		■				
Collection of data from the field through questionnaires			■			
Data processing and interpretation ready for report drafting				■		
Preparation of the first draft report					■	
Submission of the report at SLADS						■

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

APPENDEX IV.

RESEARCH REPORT BUDGETING.

ACTIVITIES	COST ANALYSIS	COST TOTAL
Local transport	50,000 per week	200,000/=
Secretarial service	20 pages@ 300x20x20	120,000/=
Stationary	5 Reams of paper A4	80,000/=
Binding	500Copies@2000 x500	100,000/=
Total	Amount	500,000/=

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz

APPENDIX V

VERICATION LETTER FOR DATA COLLECTION

TANZANIA REVENUE AUTHORITY

Ref. No.: GD.194/735/B2/02 **07th May, 2026.**

Jonathan Jackson john,
Tanzania Library Services Board School of Library,
Archives and Documentation Studies,
P.O.BOX 227,
Bagamoyo Pwani.

Re: Request for Data Collection Placement.

Please refer to your letter dated **13th April, 2026** with **REF. NO: DA.201/457/VOL/1/20**

This is to inform you that your request for data collection attachment to **TRA-Kinondoni Tax Region** has been accepted. You have been assigned to the **Tanzania Revenue Authority (TRA) – Kinondoni Tax Region** for your Data Collection, effective from **27th** March, 2026 to 11th May, 2026.

Please take note that no any **Financial Assistance/Support** will be provided to you during your stay in Kinondoni Tax Region and practical work extension, thus you are advised to observe the period stipulated for field as well as other TRA Regulations and directives issued by their supervisor.

Wishing you all the best and warmly welcome to **TRA, KINONDONI TAX REGION.**

"Together We Build Our Nation"

Faiz Mohamed
For: Regional Manager

"ISO 9001 : 2015 CERTIFIED"
Regional Manager
Kinondoni - Mwenge nearby JWTZ Flats
P.O. Box 9774, Dar es Salaam, Tanzania
Tel: +255 22 2771846, 2771859 **Fax:** +255 22 2771861, 2771869

SLADS Research Hub · SLADS/2026/00046 · repository.slads.sc.tz