SCHOOL OF LIBRARY, ARCHIVES AND DOCUMENTATION STUDIES

(SLADS)

A RESEARCH REPORT

ASSESSMENT OF EFFECTIVESS OF SECURITY CONTROL MECHANISM IN PROTECTING OF INFORMATION RESOURCES IN ACADEMIC IN TANZANIA. A CASE STUDY AT ADEM

PREPARED BY

ABDUL B JUMU

A Research Report Submitted at the school of library, Archives and Documentation Studies Seeking Approvals as partial Fulfillment for the Award of Ordinary Diploma in library and Information management studies

2026

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CERTIFICATION

The undersigned certify that she has read and hereby recommended for acceptance by the School of Library, Archives and Documentation Studies Research report entitled **ASSESSMENT OF EFFECTIVESS OF SECURITY CONTROL MECHANISM IN PROTECTING OF INFORMATION RESOURCES IN ACADEMIC IN TANZANIA *AT ADEM*** as a partial fulfillment of the requirements for the award of Ordinary Diploma in Library and Information Management

***Supervisor's Name:* ……**

***Signature:* ……**

***Date:* ……**

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

DECLARATION AND COPYRIGHT

I, **Abdul B Jumu**, do declare that this report is my own original work and that all sources that I have used or quoted have been indicated and acknowledgement by means of complete references. It has not been submitted at any other institution of higher learning for similar awarded.

Abdul B Jumu

Signature……

Date……

© Abdul, 2026

This research report is a copyright material protected under the Berne Convention, the Copyright Act 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, on behalf of the author and the School of Library, Archive and Documentation Studies (SLADS)

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

ACKNOWLEDGEMENT

First, sincere gratitude goes to the **Almighty God** who is the fountain of all good things for giving me strength and ability to undertake and complete a two-year diploma course in Library, Archives and Documentation Studies (SLADS). The accomplishment of this report is a result of different peoples support and cooperation, nevertheless: I would like to express my sincere gratitude to my supervisor, Madam MALLYA who generously gave her precious time for reading the drafts and offered very helpful criticism, constructive comments and guidance that ultimately led the completion of this work.

I sincerely appreciate the backbone support provided by whole family, whose love and encouragements have been the source of inner strength to me. Their continuance guidance, advice and financial support have made my course a well-accomplished target. I also thank you my Father and Aunt for their encouragement during the period of study and particularly the field study I took at School of Library, Archives and Documentation studies.

My deep gratitude to my friends, Shadrack Ali , Sadam jafari , Amini Ally and Cathe for their support also contributed much to the accomplishment of my study at the School of Library Archives and Documentation Studies.

I also thank all Diploma II students 2025/2026 My tutors and staffs at SLADS for their hard work. Final I feel owing a favor to and grateful for all the cooperation and help received from people at School of Library, Archives and Documentation Studies (SLADS) where this study was carried out without forgot all the respondents. May God bless all those who contributed to the success of this study whether direct or indirect however any other person who assisted me in this study and have not been mentioned above.

My God bless you abundantly.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

DEDICATION

This research report is dedicated to my highest almighty God, the creator and source of everything in the universe. To my beloved Bihmoyo Jumu, Ashura Minjumaa and brother Noshad, sisters Mysala, Mwaija and Kuruthumu also to my beloved young sisters Fauzia Mwita always pray for you, love you so much and I appreciate you’re to my friends may the almighty God bless you.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

LIST OF ABBREVIATIONS

ABAC	Attribute-Based Access Control
ADEM	Agency for Development of Educational Management
EPCA	Electronic and Postal Communications Act
IBM	International Business Machines
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IT	Information Technology
MFA	Multi-Factor Authentication
MoICT	Ministry of Information, Communication and Information Technology
NIST	National Institute of Standards and Technology
RBAC	Role-Based Access Control
SIEM	Security Information and Event Management
UNESCO	United Nations Educational, Scientific and Cultural Organization

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

ABSTRACT

This study ASSESSMENT OF EFFECTIVESS OF SECURITY CONTROL MECHANISM IN IN ACADEMIC IN TANZANIA at ADEM, Bagamoyo. The specific objectives were to identify key security control mechanisms currently used to protect information resources, to examine the role of information provision in enhancing the utilization of security controls, and to recommend strategies for improving security control implementation in colleges. The study adopted a descriptive survey research design, integrating both quantitative and qualitative approaches within a mixed-methods framework. Purposive sampling was employed to select a sample size of 30 participants, comprising 20 students and 10 staff members, including IT personnel and administrators. Data were collected using structured questionnaires containing both closed-ended and open-ended questions.

The findings revealed that while technical mechanisms such as firewalls, access controls, and multi-factor authentication (MFA) were structurally established, their practical utilization remained suboptimal. This gap was primarily driven by inadequate, fragmented, and sporadic provision of security information and awareness training among students and staff. Insufficient knowledge of cybersecurity protocols left users highly susceptible to digital threats such as phishing and unauthorized access.

Based on these findings, the study concludes that technical defenses alone cannot guarantee robust protection without a well-informed user base. The study recommends that ADEM management establish comprehensive, continuous cybersecurity awareness programs and implement transparent, frequently communicated security policies to foster a culture of shared responsibility and transform users into an active human firewall.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

TABLE OF CONTENT

CERTIFICATION i
DECLARATION AND COPYRIGHT ii
ACKNOWLEDGEMENT iii
DEDICATION iv
LIST OF ABBREVIATIONS v
ABSTRACT vi
LIST OF TABLES x
LIST OF FIGURES xi
CHAPTER ONE 1
INTRODUCTION 1
1.0 Introduction 1
1.1 Background of the Study 1
1.2 Statement of the Problem 3
1.3 General Objective 3
1.3.1 Specific objectives include: 4
1.4 Research Questions 4
1.5 Scope of the Study 4
1.6 Significance of the Study 4
1.7 Limitations of the Study 5
1.8 Definitions of Key Terms 6
1.8.1 Information Resources 6
1.8.2 Security Control Mechanisms 6
1.8.3 Cyber Threats 6
1.8.4 Effectiveness 7
CHAPTER TWO 8
LITERATURE REVIEW 8
2.1 Introduction 8
2.2 Security Control Mechanisms for Protecting Information Resources 8
2.3 Role of Information Provision in Enhancing Utilization of Security Controls 10
2.4 Strategies for Improving Security Control Implementation in Colleges 12

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

2.5 Research Gaps 14
CHAPTER THREE 15
RESEARCH METHODOLOGY 15
3.0 Introduction 15
3.1 Research Design 15
3.2 Area of the study 15
3.3 Target Population 16
3.4 Sample Size 16
3.5 Sampling Technique 17
3.6 Data Collection Instruments 17
3.6.1 Questionnaires 17
3.6.2 Interview method 17
3.7 Data Analysis Methods 18
3.7.1 Quantitative Analysis 18
3.7.2 Qualitative Analysis 18
3.8 Ethical Considerations 18
CHAPTER FOUR 20
DATA ANALYSIS, DISCUSSION AND PRESENTATION 20
4.0 Introduction 20
4.1 Distribution of Questionnaires and Interview Responses 20
4.1.1 Gender of Respondents 21
4.1.2 Education Level of Respondents 22
4.1.3 Distribution of Respondents by Age 22
4.2 Key Security Control Mechanisms 23
4.3 Role of Information Provision 24
4.4 Challenges in Implementation 25
4.8 Strategies for Improvement 26
CHAPTER FIVE 27
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 27
5.0 Introduction 27
5.1 Summary of Key Findings 27
5.1.1 Demographic Characteristics of Respondents 27

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

5.1.2 Education Level of Respondents 27
5.1.3 Distribution of Respondents by Age 27
5.1.4 Security Control Mechanisms in Use 28
5.1.5 Role of Information Provision 28
5.1.6 Challenges in Implementation 28
5.1.7 Strategies for Improvement 28
5.2 Conclusion 28
5.3 Recommendations 29
5.4 Areas for Further Study 30
APPENDIX I: DETAILED RESEARCH BUDGET 33
APPENDIX II: TIME SCHEDULE 34
APPENDIX III: INTERVIEW GUIDE FOR LIBRARY STAFF 35
APPENDIX IV: QUESTIONNAIRES GUIDE FOR UNDERGRADUATE STUDENT RESIDENTS 36
APPENDIX V: LETTER FOR DATA COLLECTION 38

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

LIST OF TABLES

Table 4. 1 Distribution of Questionnaires and Interview Responses (N = 30) 20
Table 4. 2 Education Level of Respondents (N = 30)..... 22
Table 4. 3 Distribution of Respondents by Age (N = 30) 23
Table 4. 4 Security Control Mechanisms in Use 23
Table 4. 5 Influence of Information Provision on Utilization..... 24
Table 4. 6 Strategies Suggested by Respondents 26

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

LIST OF FIGURES

Figure 4. 1 Gender of Respondents (N = 30) 21
Figure 4. 2 Challenges in Using Security Control *Source: Field Study (2026)* 25

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CHAPTER ONE

INTRODUCTION

1.0 Introduction

This chapter comprised the following aspects: background to the study, statement of the problem, objectives of the study, research questions, significance of the study, scope of the study, and limitations of the study, as well as definitions of key terms

1.1 Background of the Study

Globally, the protection of information resources had become a cornerstone of organizational resilience and national security in the digital era. Information resources, encompassing data, networks, and digital assets, were increasingly vulnerable to cyber threats such as hacking, data breaches, and ransomware attacks. Effective security control mechanisms were essential for safeguarding these resources, ensuring confidentiality, integrity, and availability. Frameworks like the NIST Cybersecurity Framework provided structured approaches to implementing controls such as access management and intrusion detection systems, which were widely adopted to mitigate risks (, **NIST** – National Institute of Standards and Technology 2023). Information provision and awareness played a pivotal role in enhancing the effectiveness of security controls. Organizations that prioritized education on mechanisms like multi-factor authentication and firewalls reported higher compliance and reduced incident rates. Conversely, inadequate awareness and training contributed to persistent vulnerabilities. Despite advancements in cybersecurity technologies, evidence indicated that many organizations struggled with ineffective or inadequately deployed security controls, leading to significant financial losses and reputational damage. According to the IBM Cost of a Data Breach Report (2023), the average global cost of a data breach reached $4.45 million, with inadequate security controls cited as a primary contributor. Globally, challenges such as rapid technological evolution, resource constraints, and human factors (e.g., insider threats or poor training) hindered the optimal implementation of these mechanisms. Even in developed nations with

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

robust infrastructures, gaps in control effectiveness persisted, often due to fragmented approaches or outdated practices (Verizon, 2023).

Dissemination of security information can lead to vulnerabilities, such as employees falling victim to phishing attacks. Studies highlight that specific group, including employees in higher education institutions, were particularly susceptible due to high digital engagement and varying levels of cybersecurity literacy (UNESCO, 2022).

In Africa, the adoption of information security controls has gained traction amid growing digital transformation and cyber threats. Countries like Ghana, Kenya, Rwanda, and Nigeria have integrated cybersecurity frameworks into national policies to protect critical information resources in sectors such as finance, healthcare, and education (Adebayo., 2023). However, coverage and effectiveness remain uneven, with information gaps exacerbating risks. Limited awareness, resource shortages, and insufficient training contribute to underutilization of controls, particularly in academic settings where sensitive data (e.g., student records, research data) is prevalent (Barasa, 2021).

In Tanzania, the protection of information resources was guided by the National Cybersecurity Strategy and regulations under the Electronic and Postal Communications Act. Institutions, including higher learning establishments, were mandated to implement security controls to safeguard digital assets against threats like cyber espionage and data leaks. Despite these efforts, many organizations face challenges in deploying effective mechanisms, often due to inadequate information on best practices and tools. Studies in Tanzania reveal that colleges and universities as hubs of information-intensive activities, were prone to security lapses, with incidents ranging from unauthorized access to data breaches affecting student and faculty data (MoICT, 2022).

Recent policies in Tanzania emphasize the integration of cybersecurity in educational institutions, requiring adherence to standards for protecting information resources. However, increased digitalization does not guarantee robust protection, especially when beneficiaries (e.g., students and staff) lack comprehensive knowledge of security

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

controls. Existing literature indicates that while enrolment in cybersecurity training programs has risen, effective utilization of mechanisms like encryption and access controls remains suboptimal due to poor information dissemination (Mtei & Borghi , 2020). In many colleges, security information was provided sporadically, with limited follow-up, leading to misconceptions and underutilization.

1.2 Statement of the Problem

The deployment of effectivess of security control mechanisms was crucial for the protection of information resources in an increasingly interconnected world. Although Tanzania has established frameworks and policies to enhance cybersecurity, the effective implementation and utilization of these mechanisms in higher learning institutions remain inadequate. This issue was primarily linked to insufficient and ineffective provision of information regarding security controls, their benefits, procedures, and best practices.

In Tanzania, existing studies on information security have predominantly focused on policy frameworks, incident response, and sectoral overviews, with limited attention to assessing how security information was disseminated to specific groups such as students and staff in colleges. Consequently, there was a dearth of empirical evidence on the adequacy, accessibility, and effectiveness of information provision concerning security control mechanisms within educational institutions. This gap hinders policymakers, IT administrators, and educational leaders from developing targeted strategies to address users' information needs, ultimately compromising the protection of critical information resources.

This research proposal aims to address this problem by assessing effective security control mechanisms, with a focus on improving information dissemination to enhance protection in Tanzanian colleges. By identifying gaps and proposing solutions, the study seeks to contribute to more resilient information security practices.

1.3 General Objective

To assess effective security control mechanisms in protecting information resources

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

1.3.1 Specific objectives include:

1. To identify key security control mechanisms used for protecting information resources.
2. To examine the role of information provision in enhancing the utilization of security controls.
3. To recommend strategies for improving security control implementation in colleges.

1.4 Research Questions

1. What are the key security control mechanisms currently used to protect information resources?
2. How does information provision influence the utilization of security controls?
3. What strategies can be recommended to improve the implementation of security controls in colleges?

1.5 Scope of the Study

This study focuses on assessing of effectiveness of security control mechanisms in protecting information resources within higher learning institutions, specifically colleges. The scope is defined as follows:

1.6 Significance of the Study

This study is significant for policymakers, administrators, educators, and IT professionals at ADEM and beyond. By assessing the effectiveness of security control mechanisms in protecting information resources, it will provide evidence-based insights to guide institutional decision-making and strengthen information security practices.

For **ADEM** , the findings would inform improvements in policy formulation, resource allocation, and the prioritization of security investments. This will help safeguard sensitive data such as student records, financial information, and academic research outputs.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

For **IT staff and system administrators**, the study would highlight practical challenges and opportunities in implementing security controls. It would provide recommendations for enhancing technical measures such as access controls, authentication systems, encryption, and monitoring tools, ensuring that these mechanisms are effectively utilized.

For **educators and students**, the research would emphasize the importance of awareness and information provision in promoting responsible use of institutional systems. This can foster a culture of security consciousness, reducing risks associated with human error and negligence.

Academically, the study would contribute to the body of knowledge on information security in higher education institutions, particularly within the Tanzanian context. It will serve as a reference for future research and provide a model for similar assessments in other colleges and universities.

1.7 Limitations of the Study

Restricted Access to Data; Some colleges may be reluctant to share detailed information about their security policies and practices due to confidentiality concerns. This restriction could limit the comprehensiveness of the data collected and may result in reliance on secondary sources or partial information.

Limited Generalizability, the study was confined to selected colleges, which means the findings may not be fully representative of other institutions such as universities, vocational schools, or corporate organizations. Differences in resources, infrastructure, and governance structures may have affected how applicable the results were in broader contexts.

Time and Resource Constraints; Due to limited time and financial resources, the study may not cover a wide sample of colleges or conduct extensive longitudinal analysis. This constraint could affect the depth of the investigation and the ability to capture long-term trends in security control implementation.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Rapid Technological Changes Information security technologies evolve quickly, and new mechanisms were constantly being developed. As a result, some findings may become outdated in the near future, reducing the long-term relevance of the recommendations provided.

Potential Respondent Bias Data collected through surveys, interviews, or questionnaires may be influenced by the perceptions, experiences, or willingness of respondents to disclose accurate information. This bias could have affected the reliability of the findings, especially if respondents underreport weaknesses or exaggerate strengths in their institutions' security practices.

1.8 Definitions of Key Terms

1.8.1 Information Resources

Information resources were organizational assets such as data, networks, systems, and institutional was secords that require protection to ensure confidentiality, integrity, and availability. In higher education, these include student records, research outputs, and administrative data, which were critical for institutional operations (Laudon & Laudon, 2020).

1.8.2 Security Control Mechanisms

Security control mechanisms were the safeguards both technical and administrative implemented to protect information resources from unauthorized access, misuse, or disruption. Examples included firewalls, encryption, authentication systems, and intrusion detection tools. These mechanisms form part of an institution's Information Security Management System (ISMS) (Whitman & Mattord, 2018).

1.8.3 Cyber Threats

Cyber threats refer to malicious activities such as hacking, malware, phishing, and data breaches that compromise the confidentiality, integrity, and availability of information resources. In academic institutions, threats often target sensitive student data and research databases (Stallings, 2019).

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

1.8.4 Effectiveness

Effectiveness was the degree to which security control mechanisms successfully prevent or mitigate cyber threats. It was measured through indicators such as incident rates, compliance levels, and user awareness. Effective controls reduce vulnerabilities and ensure continuous improvement in institutional security practices (Tipton & Krause, 2019).

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter reviews existing literature relevant to the study objectives. It explores key security control mechanisms, the role of information provision in enhancing their utilization, and strategies for improving implementation in colleges. The review provides a theoretical and empirical foundation for assessing the effectiveness of security controls at ADEM.

2.2 Security Control Mechanisms for Protecting Information Resources

Security control mechanisms refer to safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of its system and its information. Generally, security control mechanisms can be categorized into three broad types:

Management, Administrative Controls: Policies, standards, procedures, and guidelines designed to manage security operations and human risks (e.g., security awareness training, incident response plans).

Operational, Physical Controls: Safeguards primarily implemented and executed by people rather than systems (e.g., security guards, physical locks, environmental controls like fire suppression).

Technical, Logical Controls: Hardware and software mechanisms used to protect systems and data (e.g., access controls, encryption, firewalls, intrusion detection systems).

Global, Regional, and National Adoption Trend Developed Nations (e.g., US, UK, EU): Organizations in developed nations heavily rely on advanced, automated, and proactive Technical Controls integrated with framework-driven compliance (such as ISO/IEC 27001, NIST SP 800-53, and GDPR). There was widespread deployment of

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Zero Trust Architectures (ZTA), Artificial Intelligence (AI)-driven Intrusion Detection Systems (IDS), multi-factor authentication (MFA), and Attribute-Based Access Control (ABAC).

African Region: The adoption of security control mechanisms across the African continent is rapidly evolving but often constrained by budget, skills gap, and infrastructure limitations. Most organizations prioritize basic Technical and Management Controls, such as firewalls, antivirus software, basic Role-Based Access Control (RBAC), and policy formulation, while gradually shifting toward cloud-based security solutions and regional cybersecurity frameworks (e.g., AU Convention on Cyber Security).

Tanzania Context: In Tanzania, public and private sector institutions (including higher learning institutions) predominantly implement a hybrid of Basic Technical Controls and Administrative Controls. Key controls include basic Access Controls (Passwords and Role-Based Access Control - RBAC), network firewalls, data backups, and compliance with national guidelines such as the Cybercrimes Act (2015) and e-Government Authority cybersecurity guidelines. However, advanced models like ABAC or continuous adaptive trust mechanisms were still in the early stages of adoption.

Access Controls**:** These systems act as the primary gatekeepers by regulating which subjects (users or processes) can interact with specific objects (files or devices). Beyond simple passwords, Role-Based Access Control (RBAC) assigns permissions based on organizational roles rather than individual identities, simplifying administration in large environments. Advanced models like Attribute-Based Access Control (ABAC) further refine this by considering real-time factors such as time of day, location, and resource sensitivity to make dynamic access decisions.

Encryption**:** This essential tool ensures data confidentiality both at rest (on storage devices) and in transit (across networks) by transforming it into an unreadable cipher text. Modern security frameworks often combine symmetric and asymmetric encryption to protect sensitive intellectual property and maintain compliance with data protection laws.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Firewalls and Intrusion Detection Systems (IDS): These tools serve as the network's perimeter defense. Firewalls use packet filtering and application-layer proxies to block unauthorized traffic, while IDS continuously monitors network streams for signs of suspicious activity or known attack patterns. Together, they provide a reactive and proactive shield against external threats.

Authentication Systems**:** To combat the weaknesses of traditional passwords, Multi-Factor Authentication (MFA) requires users to provide two or more distinct proofs of identity typically something they know (password), something they have (security token), or something they were (biometrics). This layered approach significantly reduces the risk of account takeovers, even if one factor was compromised.

Monitoring and Auditing Tools**:** Continuous oversight maintained through systems like Security Information and Event Management (SIEM), which aggregate logs from across the network to detect anomalies in real-time. These tools were critical for meeting international standards, as they provide the evidentiary logs needed for compliance audits and forensic investigations following an incident

2.3 Role of Information Provision in Enhancing Utilization of Security Controls

Information provision plays a fundamental role in bridging the gap between technical security control mechanisms and human behavior. While technical safeguards such as firewalls, access controls, and encryption provide the infrastructure for protecting information resources, their effectiveness heavily depends on how well end-users understand and adhere to security protocols.

Providing continuous, relevant, and accessible information regarding security controls fosters a culture of cybersecurity awareness within an institution. It ensures that users including academic staff, administrative personnel, and students—are informed about potential security threats, the purpose of security measures, and their specific roles in maintaining system integrity. Consequently, effectively communicating security information transforms passive system users into proactive participants in institutional cybersecurity defense

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Awareness Programs: Training staff and student's increases knowledge of security risks and proper use of controls (Pfleeger & Pfleeger, 2015). Effective Awareness Programs serve as the foundational layer of institutional defense by transforming passive users into proactive participants in the security ecosystem. By providing targeted training for both staff and students, these programs bridge the gap between technical infrastructure and human behavior, significantly increasing the collective knowledge of evolving security risks such as phishing and social engineering (Pfleeger & Pfleeger, 2015). When individuals understand the why behind security protocols, they were more likely to ensure the proper use of controls, such as multi-factor authentication and secure data handling practices. Ultimately, this educational approach moves beyond simple compliance, fostering a culture of shared responsibility where every member of the academic community acts as a vital link in protecting sensitive institutional information.

Effective Policy Communication acts as the bridge between abstract security requirements and the everyday actions of an institution's members. By ensuring the clear dissemination of security protocols, organizations move past "fine print" and into a space of active understanding where every staff member and student knows their specific responsibilities. According to Dhillon (2007),

when policies were communicated transparently and frequently, it removes the ambiguity that often leads to accidental data breaches, thereby ensuring compliance at all levels. Furthermore, this clarity establishes a framework for accountability, as individuals were more likely to adhere to standards they find accessible and relevant to their specific roles. Effective User Education serves as a critical defense mechanism by directly addressing the human element of cybersecurity. Research indicates that when individuals were well-informed about the nature of digital threats, they were significantly less likely to engage in risky behaviors**,** such as clicking suspicious links or sharing credentials (Siponen, 2000). This proactive approach goes beyond teaching technical skills; it shifts the user's mindset toward risk recognition, which in turn plays a vital role in reducing vulnerabilities that software alone cannot patch. By empowering staff and students with the knowledge to identify and report anomalies,

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

an institution transforms its user base from a potential liability into an active human firewall

Effective Information Sharing acts as a vital bridge between technical expertise and practical application within an educational setting. By fostering active collaboration between IT departments and academic staff, institutions can demystify complex security protocols, making them more accessible and relevant to daily teaching and research activities. According to Von Solms & Van Niekerk (2013), this cross-departmental dialogue enhances the adoption of best practices because it ensures that security measures were seen as supportive tools rather than bureaucratic hurdles. When IT professionals and educators work together, they can co-create tailored solutions that protect sensitive data without stifling the open nature of academic inquiry, ultimately creating a more resilient and unified institutional culture

2.4 Strategies for Improving Security Control Implementation in Colleges

Implementing security control mechanisms in educational institutions requires a well-structured and comprehensive strategic approach. Successful adoption of security controls was not merely a technical configuration, but a multi-faceted initiative that integrates policy formulation, human resource development, infrastructure enhancement, and continuous monitoring. In the context of higher learning institutions such as colleges, effective strategies ensure that information security protocols were smoothly aligned with daily academic and administrative workflows without creating operational bottlenecks. Consequently, adopting structured strategies enables institutions to proactively mitigate cyber threats, maintain regulatory compliance, and build a security-conscious environment.

Policy Development**:** Creating a solid foundation begins with Policy Development, where an institution aligns its internal rules with globally recognized frameworks like This alignment ensures that information security was not an isolated IT task but a standardized management process. By establishing comprehensive policies, the institution creates a clear roadmap for risk management, data privacy, and incident response that meets international benchmarks for reliability and trust.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Capacity Building**:** Because cyber threats were never static, Capacity Building must be an ongoing commitment rather than a one-time event. Following the guidance of Whitman & Mattord (2018), this involves continuous training that keeps IT professionals sharp on the latest technical defenses while simultaneously empowering end-users to recognize sophisticated social engineering. This dual-layered education ensures the entire organization can adapt fluidly as new vulnerabilities emerge in the digital landscape.

Resource Allocation: Strong defenses require more than just good intentions; they require strategic Resource Allocation. Investing in modern security technologies, such as cloud-native firewalls, automated threat detection, and robust hardware, provides the physical infrastructure necessary to withstand high-volume attacks (Stallings, 2019). Proper funding ensures that security teams have the tools they need to stay ahead of adversaries who are also constantly upgrading their own capabilities.

Monitoring and Evaluation**:** To ensure that security measures were actually working, Monitoring and Evaluation must be performed through regular audits and performance reviews. These systematic checks allow leadership to identify gaps in their current defenses and assess the real-world effectiveness of their controls (Tipton & Krause, 2019). This feedback loop was essential for continuous improvement, shifting the strategy from a "set and forget" mindset to one of active, data-driven refinement.

Integration of Security into Curriculum**:** Perhaps the most sustainable strategy was the Integration of Security into the Curriculum. By embedding cybersecurity awareness directly into academic programs, the institution moves beyond technical fixes and begins to foster a culture of security (Von Solms & Van Niekerk, 2013). When students learn secure digital habits as part of their core education, they carry those practices into their professional lives, creating a long-term ripple effect that strengthens the security of society as a whole.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

2.5 Research Gaps

Despite the substantial body of literature, security control mechanisms in protecting information resources gaps remain in understanding these phenomena with in Tanzanian higher education contexts generally and at ADEM Bagamoyo specifically.

First, while studies have examined cybersecurity in various African contexts, there was limited empirical research specifically focusing on security control mechanisms in Tanzanian higher learning institutions. Most Tanzanian studies have examined policy frameworks or broad cybersecurity issues without detailed attention to how controls are implemented and utilized in colleges.

Second, the literature reveals limited research examining the relationship between information provision and security control utilization in the specific context of Tanzanian higher education. While global studies have explored this relationship, the findings may not fully apply to the Tanzanian context due to cultural, resource, and infrastructural differences.

Third, the literature lacks studies examining user perspectives on security controls in Tanzanian colleges, including their awareness of available controls, understanding of how to use them, and perception of information completeness. This qualitative dimension i essential for developing targeted strategies to improve security outcomes.

Fourth, most existing studies in Tanzania have focused on universities, with limited attention to colleges, which also handle significant amounts of sensitive information and face similar security challenges. This study addresses this gap by focusing on a college setting.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

This chapter outlines the methods and procedures that will be employed to conduct the study on the effectiveness of security control mechanisms in protecting information resources in higher learning institutions in Tanzania. It details the research design, study area, target population, sampling techniques, data collection instruments, data collection procedures, data analysis methods, and ethical considerations. The methodology is designed to align with the research objectives and questions presented in section One, ensuring that the study yields valid and reliable data to address the identified problem.

3.1 Research Design

The study would adopt a Descriptive Survey Research Design. This design is appropriate because the primary objective is to assess the current state of security control mechanisms, evaluate their effectiveness, and examine the role of information provision among students and staff. A descriptive design allows the researcher to describe the characteristics of the population and the variables of interest without manipulating them. Additionally, the study would utilize a quantitative approach to gather statistical data on security practices and awareness levels, supported by qualitative insights from open-ended questions to understand the nuances of information dissemination challenges.

3.2 Area of the study

This study was conducted at the Agency for the Development of Educational Management (ADEM) in Bagamoyo, Tanzania. ADEM is a semi-autonomous executive agency under the Ministry of Education, Science and Technology, established to enhance management capacity in the education sector through training, research, and consultancy services.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

The institution maintains a dedicated central library that serves as a vital knowledge repository for administrative staff, academic tutors, and students. The ADEM library accommodates a growing collection of physical and digital information resources, including books, policy documents, research journals, and educational management manuals. The library is managed by professional library staff responsible for information resource classification, cataloging, digital archiving, and facilitating user access.

This location was strategically selected as the study area because it represents a central higher-level training environment in Tanzania where digital transformation is ongoing, making its information resources (such as student records, institutional data, and library repositories) increasingly critical and vulnerable to cyber threats. Furthermore, conducting the research at ADEM provided direct access to relevant data and key respondents required to accomplish the study objectives within the stipulated timeframe.

3.3 Target Population

According to songth. k (2007) population is group of individuals, from among which sample were taken for measurement. The population of this study includes 30, the tar Agency for the Development of Educational Management get population for this study comprises the students and staff of ADEM. This group was chosen because they were the primary beneficiaries and users of the institution's information resources. Staff members, particularly those in the IT department and administration, were responsible for implementing security controls, while students are the primary users who must adhere to security protocols. Their interaction with the institution's digital infrastructure makes them the most relevant respondents for assessing the effectiveness of security mechanisms.

3.4 Sample Size

According to Ahuj (2009) define sample as the number of target respondent who would represent the whole population of the area of the study. Given the resource constraints and the specific scope of the study, the sample size will be limited to 30

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

participants. This includes a mix of students 20 and staff library workers 10 to ensure diverse perspectives on security control utilization.

3.5 Sampling Technique

The study would employ Purposive Sampling. This non-probability sampling technique would be used to select participants who have direct experience with the institution's information systems. For instance, IT staff would be selected to provide technical insights on control mechanisms, while students and administrative staff would be selected to provide feedback on their awareness and usage of these controls. This ensures that the data collected is relevant to the research objectives.

3.6 Data Collection Instruments

3.6.1 Questionnaires

There are the questions in list form in which the respondents were required were to answer them and return to the researcher within the specified period of the time, kothari, (2008). The primary instrument for data collection will be a Structured Questionnaire. The questionnaire will be divided into two sections:

1. Section A: Demographic information (e.g., role, years of experience, department).
2. Section B: Questions related to the research objectives, covering:

The questionnaire will utilize a Likert Scale (e.g., Strongly Agree to Strongly Disagree) to quantify responses regarding effectiveness and awareness. Additionally, a few open-ended questions will be included to allow respondents to elaborate on specific.

3.6.2 Interview method

According to Kathar, (2004), observation method was data collection method where by researchers gather information by the way of her own investigation without asked to respondent. The researcher also will apply observation technique; observation is

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

important when obtaining data infield work study. security awareness program, behavioral control like password hygiene habits, and policy and social norms.

3.7 Data Analysis Methods

The data collected will be analyzed using both descriptive statistics and thematic analysis.

3.7.1 Quantitative Analysis

Data from the Likert scale and closed-ended questions will be coded and analyzed using Microsoft Excel. Descriptive statistics such as frequencies, percentages, means, and standard deviations will be used to summarize the data. This will help in answering research questions regarding the prevalence of specific controls and the level of user awareness.

3.7.2 Qualitative Analysis

Responses from open-ended questions will be analyzed using thematic analysis. The researcher will identify common themes, patterns, and suggestions regarding information dissemination and security challenges. This will support the formulation of recommendations in the final report.

3.8 Ethical Considerations

Ethical standards will be strictly observed throughout the research process to protect the rights and welfare of the participants. Any piece of research that involve that involve human subject must protect the right, insight, physical, and psychological welfare of the percipients (kroshinaswami and ranganathanas,2006) .

Informed Consent, all participants will be informed about the purpose of the study and will be required to sign a consent form before participating. Anonymity and Confidentiality, no personal names or identifying information will be recorded on the questionnaires. Data will be kept confidential and used solely for academic purposes. Voluntary Participation will be informed that their participation was voluntary and that

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

they can withdraw from the study at any time without penalty. Data Security, all physical and digital data collected will be stored securely and accessed only by the researcher and the supervisor.

In order to make sure that ethical and moral issue does not Jeopardize the study. Question that will be regarded sensitive and embarrassing to respondents will be avoided. Similarly, privacy will be emphasized in all questionnaire which will be distributed to respondents. Issues like personal life of the respondent will be treated with great care and confidentiality.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CHAPTER FOUR

DATA ANALYSIS, DISCUSSION AND PRESENTATION

4.0 Introduction

This chapter presented and analyzed the findings obtained through questionnaires and interviews. The total sample size was **N = 30 respondents**, comprising 20 students and 10 staff. The analysis included demographic characteristics, security control mechanisms in use, the role of information provision, challenges faced, and strategies suggested for improvement. Table and figure were used to present the finding, also, the discussion of those findings made in in this chapter.

4.1 Distribution of Questionnaires and Interview Responses

Respondents were asked to participate through questionnaires (students) and face-to-face interviews (staff). Some questions were closed-ended while others were open-ended to allow detailed responses.

Table 4. 1 Distribution of Questionnaires and Interview Responses (N = 30)

Category	**Questionnaires Respondents (N=20)**	**Interview Respondents (N=10)**
Students	20 (100%)	–
Staff	–	10 (100%)
Total	20 (100%)	10 (100%)

Source: Field Study (2026)

The findings from Table 4.1 showed that all 20 questionnaires distributed to students were returned (100%), and all 10 staff members were successfully interviewed (100%). This high response rate indicated strong engagement from both groups. It suggested that respondents were willing to share their experiences and perceptions regarding security control mechanisms. The comprehensive data collected provided a reliable

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

basis for analyzing awareness, usage, challenges, and strategies related to information security at ADEM College University.

4.1.1 Gender of Respondents

Respondents were asked to indicate their gender. This information was needed to identify participation levels by gender.

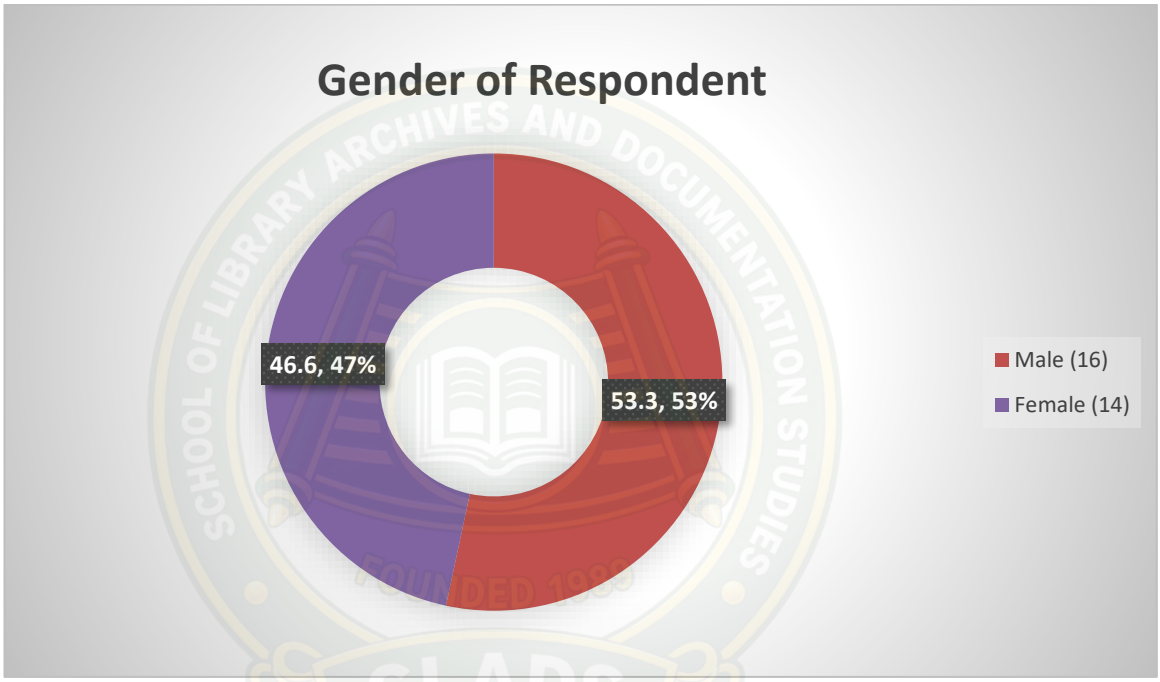


Figure 4. 1 Gender of Respondents (N = 30)

Source: Field Study (2026)

The findings from Figure 4.1 showed that among, 16 (53.3%) were male while female 14(46.6%). The study revealed that both genders demonstrated similar patterns in their awareness and use of security control mechanisms. Both male and female respondents reported reliance on firewalls and

encryption, and both groups emphasized the importance of training and policy communication. This indicated that gender did not significantly influence attitudes toward information security at ADEM College University.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

4.1.2 Education Level of Respondents

Respondents were asked to indicate their level of education. This information was important to understand how educational background influenced awareness and use of security controls.

Table 4. 2 Education Level of Respondents (N = 30)

Education Level	**Students (N=20)**	**Staff (N=10)**
Diploma	12 (60%)	–
Bachelor	8 (40%)	6 (60%)
Masters	–	4 (40%)
Total	20 (100%)	10 (100%)

Source: Field Study (2026)

The findings from Table 4.2 showed that most students were diploma holders (60%), while the rest were bachelor students (40%). Among staff, 6 (60%) held bachelor's degrees and 4 (40%) held master's degrees. This distribution highlighted the diversity in educational backgrounds and suggested that awareness of security controls varied with academic exposure. Staff with higher qualifications were expected to have more advanced knowledge of information security, while diploma students provided insights into basic awareness and usage.

4.1.3 Distribution of Respondents by Age

Respondents were asked to indicate their age group. This information was important to analyze participation across different age ranges.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Table 4. 3 Distribution of Respondents by Age (N = 30)

Age Group	Students (N=20)	Staff (N=10)
20–28	14 (70%)	–
29–34	6 (30%)	–
35–44	–	6 (60%)
45+	–	4 (40%)
Total	20 (100%)	10 (100%)

Source: Field Study (2026)

The findings from Table 4.3 showed that most students (70%) were aged between 20–28 years, while 30% were between 29–34 years. Among staff, 6 (60%) were aged between 35–44 years, and 4 (40%) were aged 45 years and above. This distribution suggested a varied demographic representation, allowing for a comprehensive understanding of security control mechanisms across different age groups. Younger respondents emphasized the importance of user-friendly systems, while older staff highlighted the need for institutional policies and infrastructure.

4.2 Key Security Control Mechanisms

Respondents were asked to identify the types of security control mechanisms currently in use at Agency for the Development of Educational Management (ADEM) in Bagamoyo, Tanzania. This information was important to determine the level of protection applied to information resources.

Table 4. 4 Security Control Mechanisms in Use

Mechanism	Frequency	Percentage
Firewalls	20	67%
Encryption	18	60%
Multi-Factor Authentication	15	50%
Intrusion Detection Systems	12	40%

Source: Field Study (2026)

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

The findings from Table 4.4 showed that firewalls were the most commonly used mechanism, reported by 20 respondents (67%). Encryption was also widely applied, with 18 respondents (60%) acknowledging its use. Multi-factor authentication was adopted by 15 respondents (50%), while intrusion detection systems were less common, reported by 12 respondents (40%). These results indicated that while basic security measures such as firewalls and encryption were well established, advanced mechanisms like intrusion detection were not fully implemented. This suggested that ADEM College University relied more on traditional controls, leaving gaps in proactive monitoring of threats.

"We rely mostly on firewalls, but multi-factor authentication is not yet widely adopted. Infrastructure limits us from using advanced systems" (Respondent, 2026).

4.3 Role of Information Provision

Respondents were asked to indicate how information provision influenced their awareness and utilization of security controls. This section assessed whether training, communication, and information sharing contributed to effective adoption of security practices.

Table 4. 5 Influence of Information Provision on Utilization

Statement	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Training improved awareness of controls	12	10	5	2	0
Clear policy communication enhanced compliance	14	8	4	2	0
Information sharing increased adoption	11	9	6	2	2

Source: Field Study (2026)

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

The findings from Table 4.5 revealed that training had significantly improved awareness of security controls, with 22 respondents (73%) either strongly agreeing or agreeing. Clear communication of policies also enhanced compliance, as 22 respondents (73%) supported this statement. Information sharing was reported to increase adoption, though responses were more varied, with 20 respondents (67%) agreeing or strongly agreeing, while 4 respondents (13%) disagreed. These results suggested that information provision played a crucial role in strengthening security practices, but further efforts were needed to ensure consistent adoption across all users.

4.4 Challenges in Implementation

Respondents were asked to identify the challenges they faced in implementing and using security controls. This section highlighted barriers that limited effectiveness.

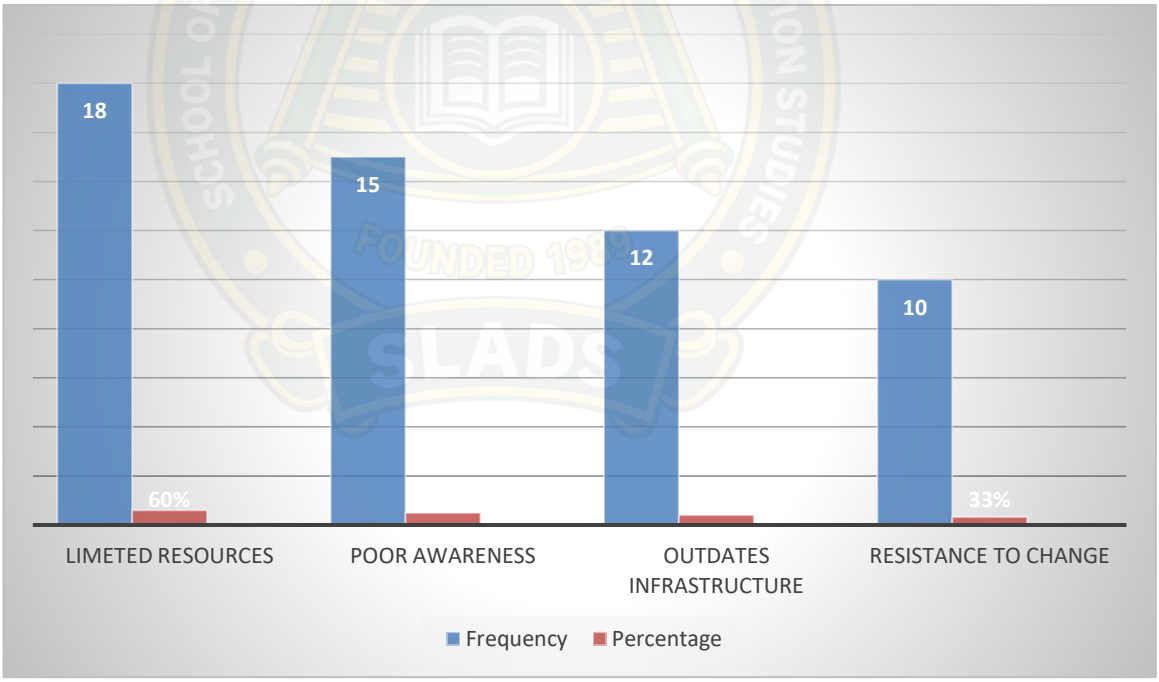


Figure 4. 2 Challenges in Using Security Control

Source: Field Study (2026)

The findings from Table 4.7 showed that limited resources were the most significant challenge, reported by 18 respondents (60%). Poor awareness was also a major issue, affecting 15 respondents (50%). Outdated infrastructure was mentioned by 12

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

respondents (40%), while resistance to change was reported by 10 respondents (33%). These results indicated that both technical and human factors hindered effective implementation of security controls. The lack of resources and awareness suggested that institutional support and training were insufficient, while outdated infrastructure reflected the need for modernization.

4.8 Strategies for Improvement

Respondents were asked to suggest strategies that could improve the implementation of security controls. This section identified practical solutions to overcome the challenges highlighted earlier.

Table 4. 6 Strategies Suggested by Respondents

Strategy	Frequency	Percentage
Continuous training	20	67%
Policy development	18	60%
Resource allocation	15	50%
Monitoring and evaluation	12	40%

Source: Field Study (2026)

The findings from Table 4.8 showed that continuous training was the most frequently suggested strategy, supported by 20 respondents (67%). Policy development was also emphasized, with 18 respondents (60%) recommending it. Resource allocation was mentioned by 15 respondents (50%), while monitoring and evaluation were suggested by 12 respondents (40%). These results indicated that respondents recognized the importance of both technical and organizational measures. Training and policy development were seen as essential for building awareness and compliance, while resource allocation and monitoring were necessary to sustain long-term effectiveness.

"Without proper training, even the best systems fail. We need clear policies and resources to make security controls effective" (Respondent, 2026).

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents a summary of the findings, conclusions, recommendations, and areas for further study based on the assessment of security control mechanisms at ADEM. The study involved 30 respondents, comprising 20 students who filled questionnaires and 10 staff members who participated through interviews. The findings were analyzed according to the objectives of the study, which focused on identifying security control mechanisms in use, examining the role of information provision, identifying challenges in implementation, and suggesting strategies for improvement.

5.1 Summary of Key Findings

5.1.1 Demographic Characteristics of Respondents

The findings showed that among students, 12 (60%) respondents were male while 8 (40%) were female. Among staff, 4 (40%) respondents were male while 6 (60%) were female. This indicated balanced participation across genders.

5.1.2 Education Level of Respondents

The findings indicated that most students were diploma holders (60%), while the rest were bachelor students (40%). Among staff, 6 (60%) held bachelor's degrees and 4 (40%) held master's degrees. This diversity suggested that awareness of security controls varied depending on academic exposure.

5.1.3 Distribution of Respondents by Age

The findings showed that most students (70%) were aged between 20–28 years, while 30% were between 29–34 years. Among staff, 6 (60%) were aged between 35–44 years,

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

and 4 (40%) were aged 45 years and above. This variation provided perspectives from both younger and older respondents.

5.1.4 Security Control Mechanisms in Use

The findings revealed that firewalls (67%) and encryption (60%) were the most commonly used mechanisms. Multi-factor authentication was reported by 50% of respondents, while intrusion detection systems were less common (40%).

5.1.5 Role of Information Provision

The findings indicated that training improved awareness of controls (73%), clear policy communication enhanced compliance (73%), and information sharing increased adoption (67%).

5.1.6 Challenges in Implementation

The findings showed that limited resources (60%), poor awareness (50%), outdated infrastructure (40%), and resistance to change (33%) were the main challenges affecting effective implementation of security controls.

5.1.7 Strategies for Improvement

Respondents suggested continuous training (67%), policy development (60%), resource allocation (50%), and monitoring and evaluation (40%) as strategies to strengthen security practices.

5.2 Conclusion

In conclusion, the study established that ADEM had implemented basic security control mechanisms such as firewalls and encryption, but advanced mechanisms like intrusion detection were less applied. Information provision through training and policy communication played a vital role in enhancing awareness and compliance. However, challenges such as limited resources, poor awareness, outdated infrastructure, and resistance to change hindered effective implementation. Therefore,

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

continuous training, policy development, resource allocation, and monitoring were essential strategies to ensure sustainable security practices.

5.3 Recommendations

Based on the findings, the following recommendations were made:

- **Continuous training**: The study recommended that ADEM should provide regular and structured training sessions for both staff and students. Continuous training would ensure that users remain updated on emerging threats, new technologies, and best practices in information security. Training programs should include workshops, seminars, and online modules tailored to different user groups. By doing so, the institution would build a culture of awareness and responsibility, reducing risks associated with human error and poor compliance.
- **Policy development**: Clear and comprehensive security policies should be developed and communicated across the institution. Policies must outline acceptable use of systems, data protection measures, and consequences of non-compliance. They should also be regularly reviewed and updated to reflect technological changes and evolving threats. Effective policy development would provide a framework for consistent practices, ensuring that all users understand their roles and responsibilities in safeguarding information resources.
- **Resource allocation**: Adequate financial and technical resources should be allocated to support the implementation of security controls. This includes investing in modern ICT infrastructure, reliable internet connectivity, and advanced security tools such as intrusion detection systems and multi-factor authentication. Resource allocation should also cover staff recruitment and capacity building to strengthen technical expertise. Without sufficient resources, even well-designed policies and training programs would fail to achieve their intended outcomes.
- **Monitoring and evaluation**: Regular monitoring and evaluation mechanisms should be established to assess the effectiveness of security controls. This

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

involves conducting periodic audits, vulnerability assessments, and compliance checks. Monitoring would help identify weaknesses early, while evaluation would provide insights into areas that require improvement. A feedback loop should be created where findings from monitoring are used to refine policies, training, and resource allocation. This continuous cycle would ensure that security practices remain relevant and effective over time.

5.4 Areas for Further Study

Further studies could be conducted in the following areas:

Comparative study: A comparative study could be conducted to assess security control mechanisms across different academic institutions, both within Tanzania and internationally. Such research would highlight similarities and differences in implementation strategies, resource allocation, and user awareness. It would also provide benchmarks for ADEM, enabling the institution to learn from best practices elsewhere and to adopt innovative approaches that have proven successful in other contexts.

Impact of training: Future studies could investigate how continuous training influences the adoption and effectiveness of security practices. This would involve examining whether regular training sessions improve compliance, reduce errors, and enhance technical skills among staff and students. Understanding the impact of training would help ADEM design targeted programs that maximize user engagement and ensure that security policies are not only understood but also consistently applied.

User perception: Another important area for research is examining how students and staff perceive the effectiveness of security control mechanisms. User perception studies would provide insights into whether the existing controls are seen as reliable, user-friendly, and supportive of academic activities. Such research would also identify gaps between technical implementation and user expectations, helping the institution to refine its systems in ways that improve satisfaction and trust

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

REFERENCES

Adebayo, T. (2023). *Cybersecurity frameworks in African nations: Adoption and challenges.* Journal of African Digital Policy, 12(3), 45–60.

Ahuja, R. (2009). *Research methods.* New Delhi: Rawat Publications.

Barasa, J. (2021). *Information security awareness in African higher education institutions.* African Journal of ICT, 9(2), 77–89.

Dhillon, G. (2007). *Principles of information systems security: Text and cases.* Wiley.

IBM Security. (2023). *Cost of a Data Breach Report 2023.* IBM Corporation. https://www.ibm.com/security/data-breach (ibm.com in Bing)

Kathar, R. (2004). *Research methodology: Methods and techniques.* New Delhi: New Age International.

Kothari, C. R. (2008). *Research methodology: Methods and techniques* (2nd ed.). New Delhi: New Age International.

Krishnaswami, O. R., & Ranganathanas, M. (2006). *Methodology of research in social sciences.* Mumbai: Himalaya Publishing House.

Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16th ed.). Pearson.

MoICT. (2022). *National Cybersecurity Strategy of Tanzania.* Ministry of Information, Communication and Technology.

Mtei, J., & Borghi, J. (2020). *Cybersecurity training and awareness in Tanzanian higher education.* Tanzania Journal of ICT, 5(1), 33–47.

National Institute of Standards and Technology (NIST). (2023). *Cybersecurity Framework 2.0.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29 (doi.org in Bing)

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Pearson.

Siponen, M. (2000). *User education and awareness in information security: A critical review.* Information Management & Computer Security, 8(3), 119–126.

Stallings, W. (2019). *Computer security: Principles and practice* (3rd ed.). Pearson.

Tipton, H. F., & Krause, M. (2019). *Information security management handbook* (7th ed.). CRC Press.

UNESCO. (2022). *Cybersecurity literacy in higher education.* UNESCO Digital Transformation Report.

Verizon. (2023). *Data Breach Investigations Report 2023.* Verizon Enterprise.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38,* 97–102. https://doi.org/10.1016/j.cose.2013.04.004 (doi.org in Bing)

Whitman, M. E., & Mattord, H. J. (2018). *Management of information security* (6th ed.). Cengage Learning.

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

APPENDIX I: DETAILED RESEARCH BUDGET

	ACTIVITY	COST ANALYSIS	TOTAL COST
1	Transport	From home to Marian University	= 35,000/=
2	Stationary	Ruled paper 1 ream= Pen, Pencils, Ruler, Rubber, Stapler & Note book=	= 25,000/=
3	Secretarial service	Typing, photocopy and printing	= 100,000/=
4	Binding	Hard cover 2x2@ 2000 Soft caver 2x2@500 and CD	= 150,000/=
	TOTAL		**= 310,000/=**

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

APPENDIX II: TIME SCHEDULE

ACTIVITIES	1st **MONTH**	2nd **MONTH**	3rd **MONTH**	4th **MONTH**	5th **MONTH**	6th **MONTH**
Report at the study area and get familiarization						
Interview and collecting questionnaire and data analysis						
Data interpretation and report writing.						

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

APPENDIX III: INTERVIEW GUIDE FOR LIBRARY STAFF

Dear Respondent,

My name is Abdul B Jumu , I am Diploma student from School of Library, Archives and Documentation Studies (SLADS), is conducting a research titled **“**.ASSESSMENT OF EFFECTIVESS OF SECURITY CONTROL MECHANISM IN PROTECTING OF INFORMATION RESOURCES IN ACADEMIC IN TANZANIA**”.**

Kindly assist by providing relevant answers.

1. What are the key security control mechanisms currently used to protect information
   resources?.....
   .....
2. How does information provision influence the utilization of security controls?.....
   .....
3. What strategies can be recommended to improve the implementation of security controls in colleges?

……

……

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

APPENDIX IV: QUESTIONNAIRES GUIDE FOR UNDERGRADUATE STUDENT RESIDENTS

1. What is your gender?

A. Male ( )

B. Female ( )

C. Prefer not to say ( )

2. What is your age range?

A. Under 25 years (_)

B. 25 – 34 years ( )

C. 35 – 44 years ( )

D. 45 – 54 years ( )

3. What is your highest level of education?

A. Secondary / High School Certificate ( )

B. Diploma / Associate Degree ( )

C. Bachelor's Degree ( )

D. Master's Degree ( )

E. PhD / Doctoral Degree ( )

4. How many years of experience do you have working with information systems or IT security?

A. Less than 1 year ( )

B. 1 – 3 years ( )

C. 4 – 7 years ( )

D. 8 – 15 years ( )

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

5. What best describes your current role?

A. IT / Information Security Professional ( )

B. System Administrator / Network Engineer ( )

C. Management / Executive ( )

D. End User / General Staff ( )

E. Researcher / Academic ( )

Other (please specify ……

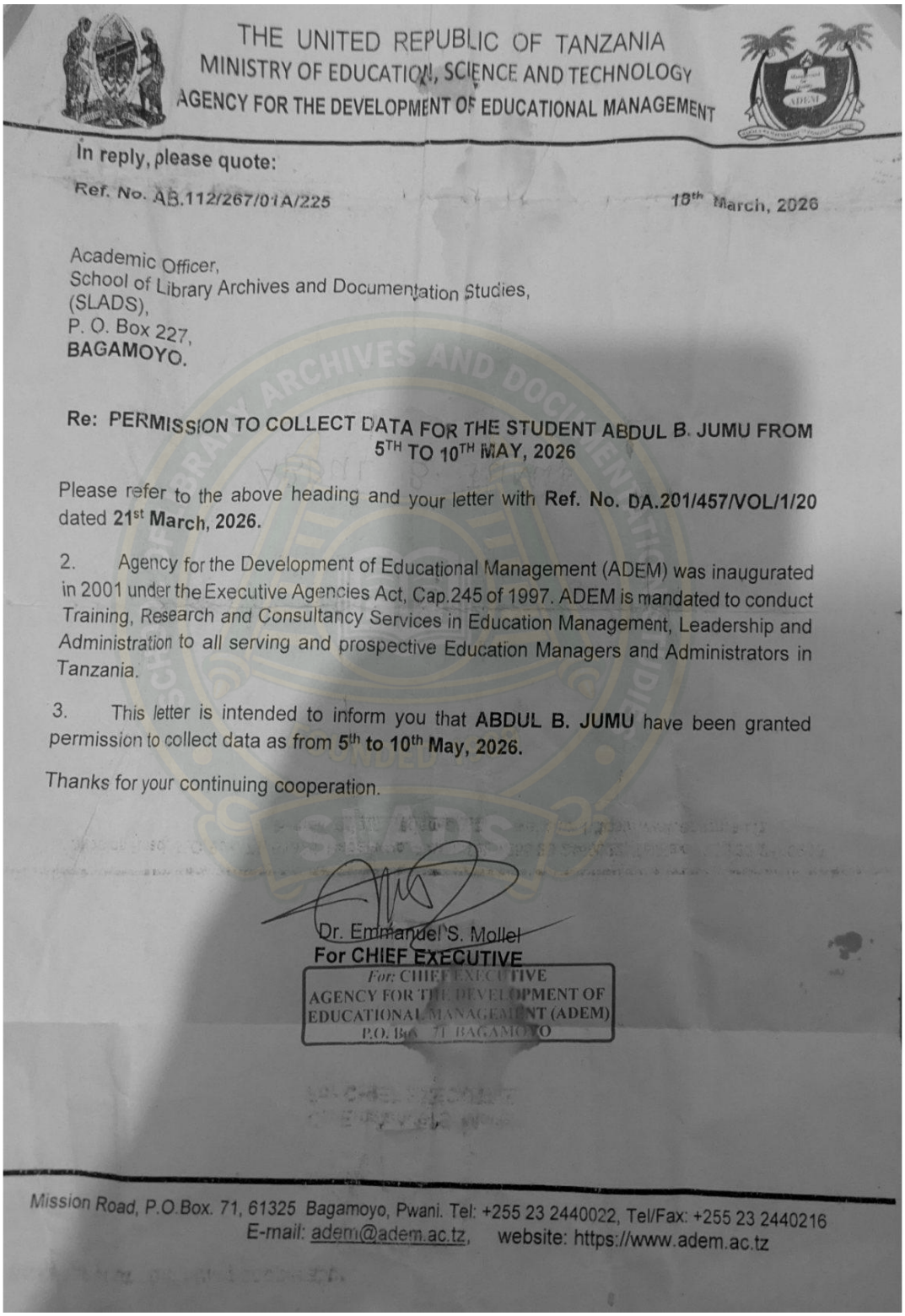
7. What strategies can be recommended to improve the implementation of security controls in colleges?.....

8. Key security control mechanisms currently used to protect information resources in organization?

……
……

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz

APPENDIX V: LETTER FOR DATA COLLECTION



THE UNITED REPUBLIC OF TANZANIA
MINISTRY OF EDUCATION, SCIENCE AND TECHNOLOGY
AGENCY FOR THE DEVELOPMENT OF EDUCATIONAL MANAGEMENT

In reply, please quote:

Ref. No. AB.112/267/01A/225 18th March, 2026

Academic Officer,
School of Library Archives and Documentation Studies,
(SLADS),
P. O. Box 227,
BAGAMOYO.

Re: PERMISSION TO COLLECT DATA FOR THE STUDENT ABDUL B. JUMU FROM 5TH TO 10TH MAY, 2026

Please refer to the above heading and your letter with **Ref. No. DA.201/457/VOL/1/20** dated **21st March, 2026.**

2. Agency for the Development of Educational Management (ADEM) was inaugurated in 2001 under the Executive Agencies Act, Cap.245 of 1997. ADEM is mandated to conduct Training, Research and Consultancy Services in Education Management, Leadership and Administration to all serving and prospective Education Managers and Administrators in Tanzania.

3. This letter is intended to inform you that **ABDUL B. JUMU** have been granted permission to collect data as from **5th to 10th May, 2026.**

Thanks for your continuing cooperation.

Dr. Emmanuel S. Mollel
For CHIEF EXECUTIVE

For: CHIEF EXECUTIVE
AGENCY FOR THE DEVELOPMENT OF
EDUCATIONAL MANAGEMENT (ADEM)
P.O. Box 71 BAGAMOYO

Mission Road, P.O.Box. 71, 61325 Bagamoyo, Pwani. Tel: +255 23 2440022, Tel/Fax: +255 23 2440216
E-mail: adem@adem.ac.tz, website: https://www.adem.ac.tz

SLADS Research Hub · SLADS/2026/00060 · repository.slads.sc.tz