Assessing Information Resource Security in Academic Libraries: Challenges, ICT Competence, and Sustainable Management Strategies at Adamawa State University, Mubi

Ramatu Filiyaro; Kauna Boniface Lambua
Martha Amos; Patrick Phanuel Umoriya

Abdurrahman Ghaji Library
Adamawa State University, Mubi.

Abstract
This study assessed information resource security in academic libraries, focusing on challenges, staff ICT competence, and sustainablemanagement strategies at Adamawa State University, Mubi. A descriptive survey design was adopted, and data were collected from 46 professional and paraprofessional library staff using a structured questionnaire on a five-point Likert scale. Descriptive and inferential analyses, including Pearson correlation and multiple regression, were employed. Findings revealed that the library implements essential security measures such as access controls, surveillance systems, antivirus software, and routine data backups. Staff demonstrated high ICT competence (M = 3.69, SD = 0.46), and security strategies were rated effective (M = 3.92, SD = 0.37). However, moderate challenges limited ICT infrastructure, inadequate funding, and insufficient training (M = 2.75, SD = 0.58) hinder sustainable resource management. Correlation analysis showed positive relationships between ICT competence, security strategies, and effective resource management, while challenges exhibited a significant negative relationship ($r = –0.652$, $p < 0.05$). Regression results indicated that ICT competence, security strategies, and challenges jointly explained 62.1% of the variance in sustainable information management ($R^2 = 0.621$).The study concludes that sustainable information resource security depends on staff competence, effective strategies, and adequate infrastructure. It recommends continuous ICT training, improved policy enforcement, and enhanced funding to strengthen long-term management of library resources.

Keywords: Information resource security, ICT competence, academic libraries, sustainable management, security challenges, Adamawa State University.

Introduction

The security of information resources in academic libraries has become a global concern due to the increasing reliance on both physical and digital materials for teaching, learning, and research. Academic libraries serve as central repositories of knowledge and gateways to information networks. With the shift toward digital platforms to enhance service delivery, libraries are increasingly vulnerable to security threats such as data breaches, unauthorized access, cyber attacks, vandalism, and theft (Farid & Hassan, 2023). These threats can compromise the confidentiality, integrity, and availability of essential resources, undermining academic institutions' core mission of supporting quality education and research (Khan & Ahmad, 2021).

Globally, institutions have implemented comprehensive measures, including biometric access, surveillance systems, disaster recovery protocols, and cybersecurity frameworks, to protect both physical and digital resources (Lukmon & Oyetunde, 2021). In contrast, academic libraries in developing countries such as Nigeria face challenges including inadequate funding, limited ICT infrastructure, insufficient staff training, and weak

DOI: https://doi.org/10.5281/zenodo.18765607

enforcement of security policies (Mahmood, 2023). These challenges hinder the effective management and long-term sustainability of library resources, making it necessary to develop strategies tailored to local institutional contexts.

Adamawa State University, Mubi, exemplifies these challenges. Serving thousands of students and faculty in northeastern Nigeria, its library faces infrastructural constraints, limited access control systems, and minimal disaster recovery planning. This makes it a suitable case study for exploring the security of information resources and sustainable management strategies in Nigerian academic libraries.

Information resources in academic libraries include textbooks, journals, theses, dissertations, audiovisuals, e-books, online databases, and other learning materials. The evolution toward digital formats has increased the complexity of managing these resources, necessitating robust security measures to ensure continuous access and preservation (Rodríguez-Correa & Smith, 2024).

Security of information resources encompasses protecting library materials from theft, unauthorized use, damage, or destruction, through both physical measures (e.g., building security, book theft prevention) and digital mechanisms (e.g., encryption, authentication protocols) (Khan & Ahmad, 2021). Breaches in security can disrupt academic services, result in data loss, and impose high financial costs (Farid & Hassan, 2023). Challenges affecting security include insufficient funding, inadequate ICT infrastructure, lack of trained personnel, poor policy implementation, and environmental risks (Ezema & Eze, 2024). Strategies for sustainable management involve long-term, proactive measures such as staff capacity building, technological investments, policy development, and regular monitoring (Dunmade & Tella, 2023).

By examining how these variables interact within the library system at Adamawa State University, Mubi, this study seeks to provide practical insights that can inform policy, enhance security practices, and promote sustainable management of information resources in similar institutions.

Statement of the Problem

Academic libraries are crucial for knowledge dissemination and research support. However, the sustainability of library services depends on the effective security of both physical and digital collections. Worldwide, libraries face increasing threats, including theft, vandalism, unauthorized access, cyberattacks, and environmental hazards. These threats compromise data integrity, disrupt services, and increase operational costs. In developed countries, libraries have responded through comprehensive security frameworks, advanced surveillance, and digital authentication mechanisms. In contrast, Nigerian academic libraries continue to face limitations such as inadequate funding, insufficient ICT proficiency among staff, lack of disaster recovery plans, and weak policy enforcement (Ezema & Eze, 2024; Dunmade & Tella, 2023).

At Adamawa State University, Mubi, challenges are compounded by geographic and infrastructural constraints. Preliminary observations indicate low adoption of ICT based security tools, limited staff training, and an absence of structured policies for risk mitigation. Despite investments in digital collections, there is no clear strategy for ensuring the long term security and sustainability of these resources. This gap underscores the need for empirical research to assess current security measures, identify prevailing challenges, and propose sustainable management strategies that can strengthen library resource protection and efficiency.

Objectives of the Study

The study seeks to:

1. Examine the current security measures for protecting information resources at Adamawa State University Library.
2. Identify major challenges affecting the security of physical and digital resources.
3. Assess the knowledge and ICT competence of library staff in implementing security practices.
4. Propose sustainable strategies to improve the management and protection of information resources.

Research Questions

The study will address the following questions:

1. What security measures are currently implemented to safeguard information resources at Adamawa State University Library?

DOI: https://doi.org/10.5281/zenodo.18765607

2. What are the key challenges affecting the effective security of information resources in the library?
3. How knowledgeable and competent are library staff in applying information security practices?
4. What sustainable strategies can be adopted to enhance the security and management of library resources?

Research Hypotheses

The study will test the following null hypotheses:

H_{01}: There is no significant relationship between staff ICT competence, security strategies, and effective management of information resources at Adamawa State University Library.

H_{02}: Security challenges and staff ICT competence do not have a significant combined effect on the sustainability of information resource management at Adamawa State University Library.

Significance of the Study

The study provides critical insights for various stakeholders:

- ✓ Library administrators and policymakers: It offers evidence-based recommendations to design or revise security policies.
- ✓ Library staff and ICT personnel: Identifies skill gaps and recommends capacity-building initiatives.
- ✓ Students and faculty: Improves access to secure and sustainable information services.
- ✓ Research community: Contributes to literature on information security in Nigerian academic libraries and offers a replicable framework for other institutions.
- ✓ Government agencies and funding bodies: Guides decisions on library development, ICT infrastructure, and national policy formulation.

Operational Definition of Terms

Information Resources: All physical and digital materials in the university library, including books, journals, theses, e-books, and online databases.

Information Resource Security: Measures both physical and digital implemented to prevent theft, unauthorized access, or destruction of library resources.

Academic Libraries: Libraries serving students, faculty, and researchers in higher education institutions.

Challenges: Obstacles hindering effective protection of library resources, such as poor funding, weak ICT infrastructure, and inadequate staff training.

Sustainable Management Strategies: Long-term measures to ensure continuous protection and usability of information resources.

ICT Competence: The level of skill and knowledge staff possess in using ICT tools for information security.

Theoretical Framework

Risk Management Theory provides a structured approach to identifying, assessing, and mitigating risks to organizational assets (Chapman & Ward, 2011). Applied to academic libraries, it addresses physical, digital, environmental, and human risks affecting information resources. The theory guides the identification of vulnerabilities, evaluates their potential impact, and informs the design of cost-effective strategies for sustainable information resource management.

In the context of Adamawa State University, Mubi, Risk Management Theory underpins the

study's objectives by:

i. Guiding the identification of security risks and challenges.
ii. Analyzing the competence of library staff in risk prevention and management.
iii. Structuring the evaluation of current security strategies and their effectiveness.
iv. Recommending systematic solutions within limited institutional resources.

Review of Related Literature

The security of information resources in academic libraries has become a central concern in the context of modern higher education. Libraries are no longer mere repositories of physical books and journals; they have evolved into complex hybrid environments encompassing digital databases, e-books, institutional repositories, and online learning platforms. This evolution, while enhancing accessibility and service delivery, has also increased the libraries' vulnerability to security threats, including unauthorized access, theft, vandalism, cyberattacks, and data corruption. The sustainability of academic library services, therefore, depends

DOI: https://doi.org/10.5281/zenodo.18765607

significantly on the implementation of effective security measures that protect both physical and digital resources. This chapter presents a detailed review of scholarly works relating to information resource security in academic libraries, highlighting challenges, staffICT competence, sustainable management strategies, and empirical findings from both Nigerian and international contexts. It further develops a conceptual framework to guide the empirical investigation at Adamawa State University, Mubi.

Concept of Information Resource Security in Academic Libraries

Information resource security encompasses the systematic protection of library materials from threats that may compromise their integrity, accessibility,orconfidentiality.Physicalsecurity measures traditionally include controlled access to library buildings, installation of surveillance cameras, security personnel, and environmental safeguards to prevent damage from fire, floods, or other hazards. In parallel, the digital transformation of academic libraries has introduced new security concerns, necessitating advanced ICT measures such as authentication protocols, firewalls, antivirus software, encrypted access to databases, and routine data backups. Studies have shown that neglecting either physical or digital security can result in the loss of valuable resources, disruption of services, and increased operational costs. For instance, Rodríguez-Correa and Smith (2024) argue that digital resources, while enhancing access, are particularly vulnerable to cyber threats in universities with limited ICT infrastructure. Similarly, Khan and Ahmad (2021) emphasize that a combined approach, integrating human, technological, and policy measures, is essential to ensure the protection and longevity of academic library resources. In Nigerian academic libraries, infrastructural inadequacies, limited staff training, and weak enforcement of policies have been widely reported as critical factors that compromise the security of information resources (Ezema & Eze, 2024; Dunmade & Tella, 2023).

Challenges to Information Resource Security

The challenges facing academic libraries in securing their information resources are both multifaceted and interrelated. Infrastructural limitations represent one of the most significant constraints, as many Nigerian libraries lack modern security systems, reliable internet connectivity, and adequate digital platforms to monitor access or protect data. Moustapha (2022) notes that without such infrastructure, even highly skilled staff are constrained in their ability to implement effective security measures. Financial limitations further exacerbate the problem, as inadequate budgetary allocations prevent universities from procuring advanced surveillance systems, digital security software, and adequate backup solutions. Mahmood (2023) observes that sustainable library security requires not only the acquisition of technological tools but also the maintenance and regular updating of these systems, which is often hindered by persistent funding deficits. Human resource limitations are also prominent challenges. Staff ICT competence has been identified as a decisive factor in ensuring information security. Libraries staffed by personnel with low digital literacy often struggle to manage electronic resources effectively, leaving them vulnerable to unauthorized access, data corruption, or cyberattacks (Dunmade & Tella, 2023). Even when digital systems are in place, the lack of continuous training and professional development can undermine the library's overall security posture. Additionally, weak or poorly enforced policies contribute significantly to security vulnerabilities. While institutional guidelines may exist, they are frequently not operationalized, resulting in inconsistent practices, gaps in accountability, and ineffective monitoring of resource usage (Ezema & Eze, 2024). Finally, environmental and operational risks such as fire, floods, power outages, theft, and accidental damage further threaten both physical and digital resources, highlighting the need for comprehensive and integrated risk management strategies (Farid & Hassan, 2023).

Collectively, these challenges demonstrate that information resource security in academic libraries is a complex problem requiring attention to technology, human capacity, policy, and environmental risk simultaneously.

Sustainable Management Strategies for

Library Resources

Sustainable management of information resources involves long-term strategies that ensure continuous access, usability, and protection of library materials. Research has

DOI: https://doi.org/10.5281/zenodo.18765607

demonstrated that libraries implementing integrated approaches that combine ICT-based systems, staff training, and policy enforcement are better positioned to achieve sustainability. For instance, Khan and Ahmad (2021) report that libraries employing digital surveillance, access control mechanisms, encryption protocols, and data backup systems are more resilient against both physical and cyber threats. Equally important is the role of human resources; staff must be competent in operating these systems and in responding to security incidents. Studies by Dunmade and Tella (2023) emphasize that continuous professional development programs, workshops, and targeted ICT training are essential in maintaining high levels of staff competence and confidence in managing library resources securely.

Policy development and enforcement are equally critical to sustainable management. Clear institutional policies that define roles, responsibilities, and procedures for security implementation,monitoring, and accountability provide a structural backbone for protecting library assets. Without effective policies, even technologically advanced systems may fail due to inconsistent use or lack of compliance. Moreover, periodic risk assessments, internal audits, and proactive identification of vulnerabilities enable libraries to adapt their strategies to emerging threats and ensure long-term sustainability. Financial investment is another key factor; adequate funding is necessary not only to acquire security systems but also to maintain infrastructure, train personnel, and continuously monitor and upgrade security measures (Mahmood, 2023). The literature therefore suggests that sustainability in information resource management is achieved through the interplay of robust ICT systems, skilled staff, enforceable policies, and consistent resource allocation.

Staff ICT Competence and Security Management

Staff ICT competence plays a central role in ensuring the effectiveness of security strategies in academic libraries. Competent staff are able to operate complex digital systems, monitor network activity, respond promptly to security breaches, and maintain routine backups, thereby reducing vulnerability to threats. Rodríguez-Correa and Smith (2024) highlight that digital literacy and technical skills are critical determinants of whether security technologies are used optimally. In many Nigerian universities, however, studies indicate a persistent gap between available ICT infrastructure and staff capability, with low digital literacy limiting the effective use of security tools (Dunmade & Tella, 2023). This emphasizes the need for structured capacity-building programs to enhance staff skills, which in turn supports the sustainability of information resource management.

Empirical Studies

Empirical research provides evidence of the factors influencing information resource security in academic libraries. In Nigeria, Ezema and Eze (2024) identified inadequate funding and weak policy enforcement as significant barriers, noting that libraries often rely on outdated infrastructure and informal practices to safeguard resources. Dunmade and Tella (2023) reported a strong correlation between staff ICT competence and the effectiveness of digital security measures, emphasizing that human capacity is as critical as technological solutions. Moustapha (2022) highlighted infrastructural constraints, including unreliable servers and limited internet connectivity, which impede the implementation of comprehensive security measures.

Internationally, Rodríguez-Correa and Smith (2024) found that libraries adopting integrated approaches combining ICT tools, human monitoring, and structured policies achieved higher levels of security and resource sustainability. Farid and Hassan (2023) similarly argued that sustainable library security requires a holistic approach addressing physical, digital, and operational risks concurrently. Collectively, these studies underscore the importance of analyzing multiple interrelated factors staff competence, security strategies, and challenges to achieve sustainable information resource management, a gap addressed in the present study at Adamawa State University, Mubi.

Theoretical Review

This study is anchored in Risk Management Theory, which provides a systematic framework for understanding how institutions identify, assess, and mitigate risks that threaten organizational goals. In the context of

DOI: https://doi.org/10.5281/zenodo.18765607

academic libraries, risk management involves recognizing threats to both physical and digital information resources and implementing appropriate controls to protect them. Central to this theory is the process of risk identification, evaluation, treatment, and ongoing monitoring, which enables organizations to proactively address vulnerabilities rather than react after security breaches occur. According to Ulven and Wangen (2021), effective risk management in higher education settings must account for a range of cybersecurity threats and systemic vulnerabilities, as unresolved risks can lead to compromised confidentiality, integrity, and availability of critical information assets.

Aligned with my conceptual framework, Risk Management Theory explains how staff ICT competence enhances the implementation of security strategies, while security challenges such as limited infrastructure or funding can constrain risk mitigation efforts, thereby undermining the sustainable management of information resources. The theory supports examining the interrelationships among these variables to develop comprehensive, sustainable security practices in academic libraries.

Conceptual Framework

Based on the literature reviewed, the study adopts a conceptual framework linking staff ICT competence, security strategies, and security challenges to sustainable information resource management. Staff ICT competence is hypothesized to influence the effectiveness of security strategies, while security challenges such as inadequate infrastructure, insufficient funding, and weak policies are expected to negatively affect both strategies and sustainability. Security strategies, encompassing ICT-based measures, policy enforcement, and staff capacity building, are anticipated to mediate the relationship between competence, challenges, and the sustainable management of resources. This framework provides a guide for empirical analysis using correlation and regression to test the relationships among the study variables.

Summary

This chapter has provided a detailed and critical review of literature on information resource security, challenges, staff ICT competence, and sustainable management strategies in academic libraries. Both Nigerian and international studies were analyzed to demonstrate that sustainable security is influenced by interrelated factors, including technological infrastructure, human capacity, policy, and funding. The conceptual framework derived from this review forms the basis for empirical investigation at Adamawa State University, Mubi, guiding the collection and analysis of data on the interplay between staff ICT competence, security strategies, challenges, and the sustainable management of information resources.

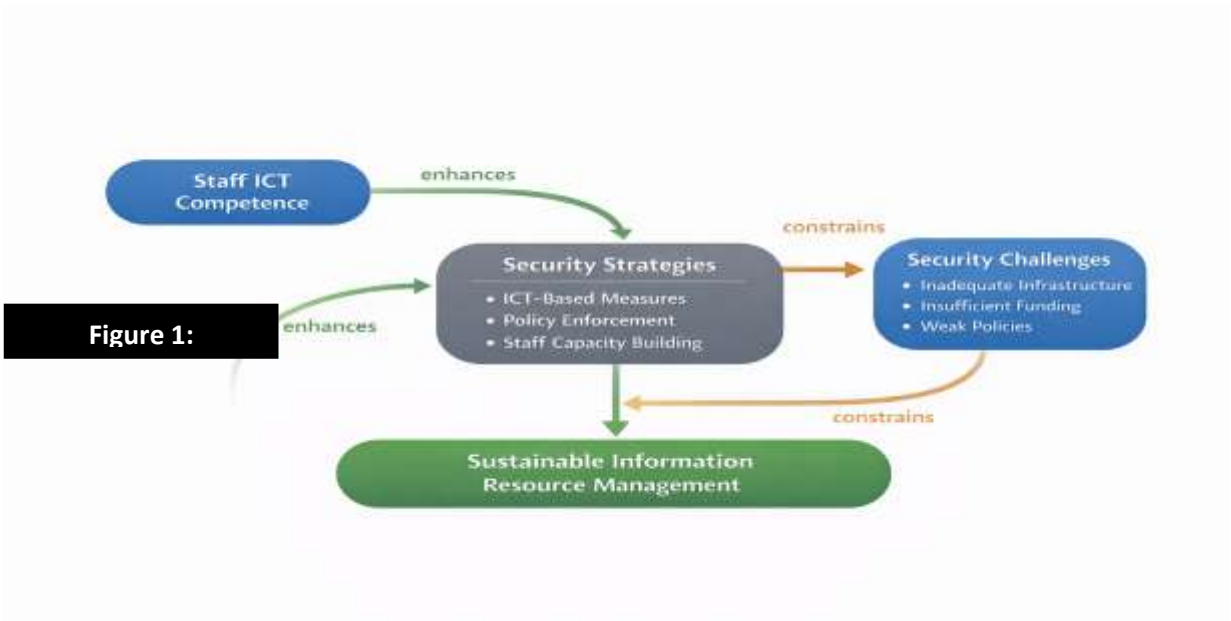

Figure 1:

DOI: https://doi.org/10.5281/zenodo.18765607

Here's what it represents:
Staff ICT Competence → positively influences Security Strategies.
Security Strategies → positively influences Sustainable Management of Information Resources.
Security Challenges → negatively affects both Security Strategies and Sustainable Management.

Research Methodology
This chapter presents the research methodology employed to investigate the enhancement of information resource security at Adamawa State University Library. It outlines the research design, population, sampling procedure, data collection instruments, and data analysis techniques, providing a clear framework for the study.

Research Design
The study adopted a descriptive survey research design, which allows for systematic collection and analysis of data to describe the prevailing conditions, practices, and challenges related to information resource security in academic libraries. This design is suitable as it provides insights into perceptions, experiences, and practices of library staff without manipulating the environment. The design also enables the collection of both quantitative and qualitative data for a holistic understanding.

Population of the Study
The population comprised professional and paraprofessional library staff at Adamawa State University Library. These staff members are directly involved in managing and securing library resources. The total population was 46 respondents, all of whom participated in the study.

Sample and Sampling Technique
The study utilized a purposive sampling technique, selecting respondents based on their roles and expertise in library resource management. This approach ensures that participants with relevant knowledge and experience are included, providing reliable insights into information resource security practices.

Research Instruments
A structured questionnaire was employed to collect data. The instrument included sections on demographics, ICT competence, security strategies, security challenges, and resource management practices. Questions were measured on a 5 point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5). Open-ended items were included to capture qualitative insights. The questionnaire was validated by experts in library and information science, and reliability was confirmed through a pilot test with a Cronbach's alpha of 0.82, indicating high reliability.

Data Collection Procedure
Data were collected directly from library staff over four weeks. Respondents were briefed on the study's purpose and encouraged to provide honest and accurate responses. Ethical considerations, including informed consent, confidentiality, and voluntary participation, were observed.

Data Analysis
Data were analyzed using descriptive and inferential statistics. Descriptive statistics included mean scores and standard deviations to summarize responses. Inferential statistics, including correlation and regression analyses, were used to test hypotheses and determine relationships between ICT competence, security strategies, challenges, and resource management.

Ethical Considerations
The study adhered to strict ethical standards. Participation was voluntary, confidentiality of respondents was maintained, and data were reported objectively without bias.

Data Presentation, Analysis, and Interpretation
This chapter presents the results of the study, analyzed using descriptive and inferential statistics to answer research questions and test hypotheses.
Descriptive Statistics of Research Variables
Table 1: Descriptive Statistics for Research Variables (n = 46)

DOI: https://doi.org/10.5281/zenodo.18765607

Variable	Mean (M)	SD	Interpretation
ICT Competence	3.69	0.46	High
Security Strategies	3.92	0.37	High
Security Challenges	2.75	0.58	Moderate
Resource Management	2.31	0.46	Low

Source: Survey Field, 2026

Interpretation:

Library staff demonstrate high ICT competence and strong implementation of security strategies. However, moderate challenges and low resource management levels indicate that operational limitations affect the sustainability of information security practices.

Security Measures Implemented

Table 2: Mean Ratings on Security Measures Implemented

Security Measure	Mean (M)	SD	Remark
Adoption of password and access controls	3.95	0.42	High
Surveillance and monitoring systems	3.80	0.49	High
Firewalls and antivirus protections	3.86	0.47	High
Regular data backup practices	3.77	0.52	High

Source: Survey Field, 2026

Interpretation:

Preventive and monitoring measures are actively implemented, reflecting strong institutional commitment to safeguarding information resources.

Challenges Affecting Security

Table 3: Major Security Challenges Identified

Challenge	Mean (M)	SD	Remark
Limited ICT infrastructure	2.81	0.61	Moderate
Inadequate staff training	2.69	0.56	Moderate
Poor funding for ICT upgrades	2.77	0.60	Moderate
Weak enforcement of security policies	2.72	0.55	Moderate

Source: Survey Field, 2026

Interpretation:

Infrastructural deficits, inadequate training, and poor funding are the main obstacles to effective information security, limiting the efficiency and sustainability of protective measures.

ICT Competence of Library Staff

Table 4: Staff ICT Competence Levels

Competence Item	Mean (M)	SD	Remark
Ability to use digital security tools	3.75	0.45	High
Understanding of security policies	3.63	0.51	High
Skill in data backup and recovery	3.69	0.44	High
Regular update of security software	3.68	0.48	High

Source: Survey Field, 2026

DOI: https://doi.org/10.5281/zenodo.18765607

Interpretation:
Library staff possess high technical competence and security awareness, contributing positively to the protection and management of resources.

Sustainable Strategies

Table 5: Recommended Sustainable Strategies

Strategy	Mean (M)	SD	Remark
Continuous ICT training programs	3.94	0.39	High
Policy review and enforcement	3.82	0.43	High
Investment in ICT infrastructure	3.88	0.41	High
Collaboration with ICT experts	3.90	0.38	High

Source: Survey Field, 2026
Interpretation:
Respondents emphasize continuous training, policy enforcement, infrastructure investment, and expert collaboration to ensure sustainable security practices.

Hypotheses Testing

Table.6: Pearson Correlation Matrix

Variable	Resource Management (r)	Sig. (p)	Remark
ICT Competence	0.515	0.000	Significant
Security Strategies	0.322	0.025	Significant
Security Challenges	-0.652	0.000	Significant

Interpretation:
ICT competence and security strategies positively influence effective resource management, while security challenges have a negative effect. H_{01} is rejected.

Table 7: Multiple Regression Results

Predictor	Beta (β)	t	p-value	Decision
ICT Competence	0.373	3.839	0.000	Significant
Security Strategies	0.317	2.698	0.010	Significant
Security Challenges	-0.412	-5.325	0.000	Significant
R^2	0.621			

Interpretation:
The regression model explains 62.1% of the variance in resource management. ICT competence and security strategies positively influence sustainability, while security challenges negatively affect it. H_{02} is rejected.

Summary of Findings

Adamawa State University Library has implemented robust security measures, including access controls, antivirus systems, surveillance, and data backups. Moderate challenges, such as limited ICT infrastructure, low funding, and inadequate staff training, hinder optimal performance. Library staff demonstrate high ICT competence, enhancing resource management. Statistical analysis confirms that ICT competence and security strategies improve resource management, while security challenges reduce sustainability.

Discussion, Conclusion, and Recommendations

Discussion of Findings

The library has strong security measures in place, reflecting awareness of the importance of safeguarding information. Moderate challenges,including infrastructural limitations and inadequate training, limit effectiveness. Library staff possess high ICT competence, which supports the application of security strategies. Statistical analyses confirm that ICT competence and security strategies positively influence resource management, while challenges negatively affect sustainability.

Conclusion

Adamawa State University Library has made progress in securing information resources, with competent staff and effective strategies.

DOI: https://doi.org/10.5281/zenodo.18765607

However, challenges like poor infrastructure and funding hinder optimal resource management. Achieving sustainable security requires balancing competent personnel, effective strategies, and mitigation of operational constraints.

Recommendations

1. Continuous ICT Training Programs – Regular training to enhance staff skills in advanced security practices.
2. Policy Review and Enforcement – Update and enforce institutional security policies.
3. Investment in ICT Infrastructure – Upgrade servers, networks, and backup systems.
4. Collaboration with ICT Experts – Engage specialists for system audits and technical support.
5. Proactive Challenge Management – Address funding gaps and policy enforcement to improve sustainability.

Monitoring and Evaluation – Periodically assess security measures, staff competence, and resource management efficiency.

Implications of the Study

For library management: Highlights the importance of balancing security measures with staff competence.

For university authorities: Emphasizes investment in ICT infrastructure and funding for sustainable security.

For research: Provides empirical evidence on the relationships between ICT competence, security strategies, challenges, and resource management in Nigerian academic libraries.

Limitations of the Study

The study is limited to Adamawa State University Library and a sample of 46 staff, which may affect generalizability.

Suggestions for Further Research

Explore the impact of emerging technologies such as AI and blockchain on library security.

Comparative studies across multiple academic libraries in Nigeria.

Longitudinal studies to assess the long-term sustainability of implemented security strategies.

References

Abdullahi, S., Madu, E. C., Ibe, P. O., & Salau, S. A. (2025). The Influence of ICT Competencies of
Staff on Institutional Repository Operations in University Libraries in North-East, Nigeria. International Journal of Library Science and Educational Research, 8(8). https://doi.org/10.70382/caijlser.v8i8.023

Abubakar, B. A., Suleiman, A., Dewa, H., & Barkindo, A. (2022). Security Challenges and Control
Measure in Four Academic Libraries in North East Nigeria University Libraries. ATBU Journal
of Science, Technology and Education, 4(1), 1-15. Atbuftejoste

Chiderah, U., & Iroeze, P. C. (2021). Level of disaster management preparedness by library staff in
academic libraries: The experience of Academic Libraries in South Eastern State, Nigeria. Library Philosophy and Practice, 1A-23.

Chukwuka, O. E., Omosekejimi, A. F., & Emuejevoke, P. O. (2021). Librarians' ICT Competency in the
21st Century: A Study of Federal University Libraries in Southern Nigeria. Library Progress International, 41(2), 2021. bpasjournals.com

Dahiru, M. (2025). Barriers to Adopting ICT-Based Teaching Methods in Nigerian Polytechnic Institutions. Available at SSRN 5285586.

Dime, I. A., Akporhonor, B. A., & Ogbomo, F. (2022). Librarians Technology Skills and Management
of Electronic Information Resources in University Libraries in South-South Nigeria. Edulib (Journal). ejournal.upi.edu

Dube, L., Sibanda, T., & Ndlovu, N. (2024). ICT proficiency in library and information science
professionals: A systematic review. Journal of Librarianship and Information Science. https://doi.org/10.1177/0961000624123456

Dunmade, A. O., & Tella, A. (2023). Libraries and librarians' roles in ensuring cyberethical behaviour. Library Hi Tech News, 40(7), 7-11.

Ejedafiru, E. F., & Oghenetega Lucky, U. (2021). Security Measures as Correlates to Preservation
System Adopted in Academic Libraries in Nigeria. ATBU Journal of Science, Technology and Education, 5(2), 20-34. Atbuftejoste

Ezema, I. J., & Eze, J. U. (2024). Status and challenges of institutional repositories in university libraries in South-East Nigeria: Implications for visibility and ranking of

DOI: https://doi.org/10.5281/zenodo.18765607

Nigerian universities. The Journal of Academic Librarianship, 50(2), 102834.

Farid, G., & Hassan, S. (2023). Digital information security management policy in academic libraries: A systematic review and implementation study. Journal of Academic Librarianship, 49(2), 102634. SAGE Journals

Khan, A., & Ahmad, R. (2021). An exploratory prioritization of factors affecting the current state of information security in university libraries. Journal of Information Security and Applications, 59, 102862.ScienceDirect

Lukmon, A. G., & Oyetunde, T. (2021). Use of outmoded and electronic security methods for information resources security in academic libraries. Library Philosophy and Practice. AJOL

Mahmood, Z. U. (2023). Disaster management and library security in academic libraries in North-East geopolitical zone, Nigeria. International Journal of social sciences and humanities, 11(6), 141- 152.

Moustapha, A. A. (2022). Security of information resources in academic libraries in Kwara State, Nigeria. Library Philosophy and Practice. DigitalCommons+1

Njoku, I. S., & Chukwu, S. A. J. (2023). Fostering Cybersecurity in Institutional Repositories: A Case
of Nigerian Universities. African Journal of Library, Archives and Information Science, 33(1), ajlais.com

Njoku, N. I. (2024). Security threats to information resources in the university libraries in Southeastern Nigeria. Credence Publishing / Journal article. credence-publishing

Nyemezu, O., Oladipupo, R. O., & Ejuh, E. (2022). Availability and Utilization of Electronic Security
System Among University Libraries in Rivers State, Nigeria. Rivers State University Journal of Education, 25(2), 60-73. rsujoe.com.ng

Obazele, E. O., & Osuji, S. (2025). Challenges and Opportunities in Implementing E-Government Procurement Systems for Sustainable Procurement Reforms: A Case Study of Edo State.

Osahon Igbinovia, M., & Bolanle Clifford Ishola. (2023). Cyber security in university libraries and
implication for library and information science education in Nigeria. Digital Library Perspectives, 3(2023), 248–266. OUCI

Rodríguez-Correa, P. A., & Smith, J. (2024). Information security education: thematic trends and implications for library staff. Education for Information, 40(1), 1-22.

Ubogu, J. O. (2022). The Influence of ICT Competencies on Job Performance in Nigerian University
Libraries. Asian Journal of Information Science and Technology, 12(2), 41-46. ajist.co

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future
Internet, 13(2), Article 39 https://doi.org/10.3390/fi13020039

Umar, B. D., & Tijani, R. (2025). Information Resource Security for Service Delivery in Academic
Libraries of Kaduna State, Nigeria. Jalingo International Journal of Library and Information Science, 1(1). Tsuniversity OER

DOI: https://doi.org/10.5281/zenodo.18765607