Journal of Applied Social Sciences and Humanities

https://journal.krrishpub.com/index.php/jassh/index

Journal of Applied Social Sciences and Humanities

# Risk Management and Security of Digital Collections: A Case Study of The University of Jos Library

Ezinne Hope Benneth [a,*], Dirmun Dimlong [b]

[a] *Department of Social Science Education, Faculty of Education, University of Jos, P.M.B. 2084, Jos, Plateau State, 930211, Nigeria.*
[b] *University Library, Federal University of Education, P.M.B. 1027, Pankshin, Plateau State, 933105, Nigeria.*

## Abstract

Academic libraries increasingly rely on digital collections to support teaching, learning, and research, yet these assets face growing risks that threaten their availability, integrity, and security. This study examines risk management and security practices in the University of Jos Library, Nigeria, focusing on existing measures, their effectiveness, technologies in use, and staff capacity. Guided by the Collection Security Management Model (CSMM), a descriptive survey design was adopted using total enumeration of 125 professional and paraprofessional staff. Findings from 67 valid responses indicate strong adoption of physical safeguards such as CCTV cameras, fire-safety alarms, and access control systems. However, procedural mechanisms and advanced digital protections remain limited, particularly in incident-response readiness, regular risk assessment, policy awareness, and staff training. The study concludes that while baseline safeguards exist, gaps in governance, technology, and human capacity undermine sustainable protection of digital collections. Recommendations emphasize institutionalized risk assessment, policy enforcement, deployment of advanced security technologies, and continuous capacity building.

*Keywords:* Academic libraries, Digital collections, Information security, Risk management, Collection Security Management Model, Cybersecurity.

**Article Information:**
DOI: https://doi.org/10.71426/jassh.v1.i1.pp37-47
Received: *25 November 2025* | Revised: *22 December 2025* | Accepted: *31 December 2025*

## 1. Introduction

Academic libraries constitute the intellectual heart of higher education institutions, supporting teaching, learning, and research by providing access to authoritative and curated information resources [1] . Through their collections and services, universities advance knowledge creation and dissemination among students and faculty [2]. Library collections serve as the bedrock upon which academic services are delivered, enabling scholarly inquiry and innovation. Ref [3] describes the academic library as a centralized environment where emerging information technologies are integrated with knowledge resources in a user-focused, service-rich setting that aligns with contemporary educational and social learning patterns.

Globally, academic libraries are rapidly digitizing their collections to enhance accessibility, preserve information resources, and support education and research activities. The Digital Library Federation conceptualizes a digital library as a distributed information system that ensures reliable storage and effective use of heterogeneous electronic resources such as text, graphics, audio, and video through global data transfer networks in a manner convenient to end users [4]. Digitization has thus transformed libraries from physical repositories into dynamic digital knowledge hubs.

Digital collections in academic libraries comprise information resources stored in electronic formats, allowing simultaneous access by multiple users irrespective of physical location. These collections are supported by complex software systems consisting of front-end applications, databases, and back-end servers that deliver services virtually to students, lecturers, and researchers. Many university libraries deploy institutional websites and repositories where theses, dissertations, scholarly publications, and creative works are preserved and disseminated digitally [5]. However, irrespective of their service orientation, all organizations including libraries are inherently exposed to risks. Shenkir et al. [6] caution that mismanagement of risk can impose severe economic and operational consequences on

[*] Corresponding author
*Email address:* 2022PGED0417@unijos.edu.ng, bennethezinnehope@gmail.com (Ezinne Hope Benneth), dirmun.dimlong@fuep.edu.ng, dirmundimlong@gmail.com (Dirmun Dimlong).

any organization.

Risk management across all levels of university library operations should therefore be accorded high priority. With the rapid advancement of information technologies, libraries, archives, and information centres increasingly create and manage resources in digital form [7]. Consequently, risk management and the security of digital collections have emerged as critical concerns within the field of library and information science [8], [9]. Universities worldwide have adopted digital technologies in their libraries, resulting in the development of digital libraries, institutional repositories, and specialized digital collections [10]. These collections encompass electronic journals, databases, e-books, multimedia resources, and digitized textual materials equipped with advanced cataloguing and retrieval functionalities.

Despite these benefits, reliance on digital technologies exposes academic libraries to cyber threats that target the accessibility, availability, and integrity of digital collections. The authors of ref [11] note that all organizations encounter risks—some predictable and manageable, others unpredictable and uncontrollable. In academic libraries, critical components such as databases are susceptible to environmental disruptions, human error, and system failures, as highlighted in reports by the National Institute of Standards and Technology [12], [13]. It is therefore imperative that library managers understand risks and adopt effective management strategies to reduce exposure to acceptable levels. Risks may arise internally through operational processes or externally through environmental and technological influences beyond managerial control [10]. Effective identification and mitigation of such risks require institution-wide awareness and coordinated action.

Ref [14] asserts that risk management is a core managerial function aimed at safeguarding organizational assets, personnel, and resources from physical and financial loss. It involves systematic identification, assessment, and mitigation of exposures using tools such as policy controls, insurance mechanisms, and technological safeguards [15]. University libraries are exposed to various risks, including operational, environmental, information technology, and compliance-related risks. Documented cases of security breaches and system failures underscore the need to integrate risk management and library security into strategic management frameworks [16].

Common risks associated with the security of digital collections include data breaches, malware attacks, phishing and social engineering, third-party vulnerabilities, and data loss or corruption. Data breaches occur when unauthorized individuals gain access to sensitive information, potentially exposing personal data and research materials [1]. Malware attacks—such as viruses, worms, and ransomware—pose significant threats by encrypting data and disrupting access to digital resources. Libraries are particularly vulnerable due to their reliance on public access networks, electronic catalogues, and shared computing infrastructures [17]. Phishing and social engineering attacks exploit human vulnerabilities by impersonating trusted entities to obtain sensitive credentials or system access [13].

Third-party risks arise when digital collections depend on external vendors for hosting, storage, or content management services. Weak security practices among these partners can introduce vulnerabilities into library systems [18]. Similarly, accidental data loss or corruption may result from hardware failures, software errors, power outages, natural disasters, or human negligence in the absence of robust backup and recovery mechanisms [19]. High-profile ransomware incidents, such as attacks on major national libraries, demonstrate the severe consequences of inadequate digital security preparedness [20], [22].

The University of Jos Library, established in 1955, serves as the central information resource of the University of Jos. Housing over 1.2 million volumes alongside extensive electronic resources, the library has embraced ICT to advance learning and research. Its digital collections are managed by system unit librarians responsible for electronic databases, institutional repositories, and online services. Given the scale and value of these resources, effective risk management and security measures are essential to ensure uninterrupted access and long-term preservation.

### *1.1. Statement of the problem*

Over the years, academic libraries have faced increasing challenges in securing their digital collections against diverse risks, including natural disasters, power failures, cyber-attacks, data loss, and human-induced threats. The University of Jos Library continues to generate and collect digital information in multiple evolving formats, each requiring specialized management and security controls. Although access control mechanisms are in place, challenges such as insufficient cybersecurity infrastructure, outdated risk management protocols, unauthorized access, and limited funding for advanced technologies threaten the integrity and availability of digital assets.

Recent developments in cyberspace have further exposed vulnerabilities related to administrative privilege abuse, inadequate software updates, and weak security governance. These challenges necessitate a comprehensive review of existing risk management practices to ensure effective protection of digital collections.

### *1.2. Aim and objectives of the study*

#### *1.2.1. Aim*

The study focuses on risk management and security of digital collections in the University of Jos Library, Plateau State, Nigeria.

#### *1.2.2. Specific Objectives*

The specific objectives of the study are to:

1. Identify existing risk management practices adopted in the University of Jos Library.
2. Ascertain the effectiveness of risk management practices in securing digital collections.
3. Examine the technologies in place and the level of digitization within the system unit.
4. Assess staff capacity and training related to digital collection management.

### 1.3. Research questions

The study seeks to answer the following research questions:

1. What risk management practices are currently in place for digital collections at the University of Jos Library?
2. How effective are the existing measures in addressing common risks in academic libraries?
3. What technologies are used to mitigate risks in the University of Jos Library?
4. To what extent is staff capacity building and training provided for managing digital collections?

### 1.4. Significance of the study

This study provides critical insights into managing risks and securing digital collections within academic libraries. The findings will enhance institutional capacity for protecting digital resources, inform policy formulation, and contribute to global best practices in digital collection management. Academic librarians, library administrators, university management, researchers, students, IT personnel, policymakers, and government agencies stand to benefit from evidence-based recommendations aimed at strengthening cybersecurity, improving staff competencies, and ensuring sustainable access to digital scholarly resources.

## 2. Theoretical framework

This study is anchored on the *Collection Security Management Model (CSMM)*, originally proposed by Da Veiga and Eloff in 2007 and widely applied in library and information science research to explain holistic approaches to collection security. The CSMM conceptualizes library collection security governance by likening it to a secured house: even when sophisticated alarm systems are installed, security can still be compromised if fundamental controls such as locking doors are neglected. This analogy emphasizes that security mechanisms alone are insufficient without responsible human behaviour and effective organizational processes [9].

The CSMM demonstrates that security measures become ineffective when the behaviour of individuals within the organization is indifferent toward implementing policies and minimizing risks at all operational levels. The model integrates five interdependent dimensions: *governance, processes, people, physical environment, and technology,* all of which carry equal weight in ensuring the confidentiality, integrity, and availability of library collections at acceptable levels [9]. Failure in any one dimension weakens the overall security posture of the library.

### 2.1. Governance perspective

Governance within the CSMM refers to the establishment of defined roles, responsibilities, policies, and practices enforced by the library's security management team. This framework ensures that strategic objectives are clearly articulated, implemented, and monitored while risks are systematically identified and mitigated. The governance dimension underscores collection security as a core managerial responsibility rather than a peripheral operational concern [21].

Effective governance requires academic libraries to develop clear risk management strategies that articulate institutional vision, priorities, and control mechanisms. These strategies include the formulation of security policies, enforcement of compliance, and continuous evaluation of risks associated with digital and physical collections. Regular risk assessments involve documenting library assets, determining their value, identifying threats and vulnerabilities, and estimating the potential cost of loss or damage [22]. Such structured governance ensures proactive rather than reactive responses to security challenges.

### 2.2. Operational process perspective

The operational process dimension focuses on the implementation of security policies and programmes through core library departments. These include acquisition, circulation, cataloguing, technical services, and special collections units. Each department plays a critical role in safeguarding collections through standardized workflows, access controls, and monitoring mechanisms [14].

For instance, acquisition units ensure secure procurement and licensing of digital resources, while circulation units regulate access and usage. Technical and cataloguing departments are responsible for metadata integrity and system configuration, and special collections units focus on preservation and conservation activities. The effectiveness of collection security is therefore dependent on the consistent execution of security protocols across all operational processes [27].

### 2.3. People perspective

The people dimension addresses the human element of collection security. It emphasizes the importance of staff competence, awareness, and accountability in implementing security measures. This includes continuous training and retraining programmes to ensure that library staff understand security policies, procedures, and incident response mechanisms [15].

The CSMM stresses the need to define clear security roles and responsibilities, supervise staff performance, and monitor adherence to established protocols. Trained personnel are better equipped to detect anomalies, report incidents accurately, and respond effectively to security breaches. Human negligence or lack of awareness can undermine even the most advanced technological safeguards, making staff capacity building a critical component of risk management [17].

### 2.4. Physical and technological perspectives

The physical and technological dimensions of the CSMM encompass both the environmental and technical mechanisms used to secure library collections. The physical environment includes the architectural design of library buildings, control of entry and exit points, surveillance systems, fire detection, and environmental controls that protect collections from physical damage [19].

The technological aspect focuses on electronic security systems and digital controls employed to prevent, detect, and respond to security threats. These include electronic anti-theft devices, surveillance cameras, access authentication systems, firewalls, intrusion detection systems, and alarm installations at strategic points within the library [19]. In digital environments, technological safeguards also extend to encryption, authentication protocols, system monitoring tools, and backup infrastructures.

Together, the physical and technological dimensions ensure both tangible and intangible assets are protected. However, the CSMM emphasizes that technology alone cannot guarantee security unless it is supported by sound governance, efficient processes, and informed personnel [8].

### *2.5. Relevance of the CSMM to the study*

The CSMM provides a comprehensive framework for examining risk management and security of digital collections in the University of Jos Library. By evaluating governance structures, operational processes, staff capacity, physical safeguards, and technological controls, the model enables a holistic assessment of existing security practices. This framework guides the identification of gaps and informs recommendations for strengthening institutional resilience against risks threatening digital collections.

## 3. Methods and procedure

This section describes the methods and procedures adopted for the study. It covers the research design, population and sample, sampling technique, instrument for data collection, validity and reliability of the instrument, procedure for data collection, and method of data analysis.

### *3.1. Research design*

Research design provides the structural framework that guides the investigation of a research problem and the achievement of stated objectives. This study adopts a *descriptive survey research design*. A descriptive survey is a quantitative approach that involves the systematic collection of data from a defined population at a specific point in time in order to describe existing conditions, attitudes, or practices [23]. This design is particularly appropriate for the present study as it enables the researcher to obtain empirical evidence on existing risk management and digital security practices in the University of Jos Library.

Surveys are especially useful where direct observation is impractical or restricted, and where respondents' perceptions and experiences are central to the research problem [24]. Quantitative survey methods facilitate the collection and analysis of numerical data through structured instruments such as questionnaires, allowing for objective measurement and statistical interpretation. In academic libraries, risk management and digital security practices are dynamic, influenced by technological change, institutional policies, and staff competencies. Descriptive surveys are therefore suitable for documenting current conditions with the aim of informing policy decisions and institutional improvements [15].

The adoption of this design aligns with the objectives of evaluating existing risk management practices, assessing the effectiveness of security measures, identifying technologies used for risk mitigation, and examining staff capacity in securing digital collections at the University of Jos Library.

### *3.2. Population and sample*

This subsection outlines the study population and explains how the sample was derived, including the rationale for its selection and its relevance to the research objectives.

#### *3.2.1. Population*

The population of a study refers to the entire group of individuals or entities from which data can be collected to answer the research questions [24]. Population may include all individuals sharing common characteristics relevant to the phenomenon under investigation [25]. The population of this study comprises all professional and paraprofessional staff of the University of Jos Library, including academic librarians, system librarians, library officers, and library assistants.

These staff categories constitute the core workforce responsible for managing, securing, and preserving digital collections. Academic librarians are primarily involved in collection development, information organization, user education, and research support, while system librarians oversee the technological infrastructure supporting digital resources. Paraprofessional staff handle daily operational activities such as circulation, cataloguing, and user assistance. Their inclusion is essential because they are often the first to identify operational risks and system anomalies [4].

In total, the population consists of 125 staff members. This population was selected because of its direct involvement in digital collection management and its relevance to examining institutional risk management practices from both human and technological perspectives.

#### *3.2.2. Sample*

A sample is a subset of the population selected for participation in a study, with the intention of making valid conclusions about the entire population [26]. In this study, the entire population of 125 staff members of the University of Jos Library constitutes the sample. This approach is feasible due to the manageable size of the population and ensures comprehensive coverage of all staff involved in digital collection management.

Using the entire population strengthens the robustness of the findings by capturing diverse perspectives across professional roles and responsibilities. It eliminates the risk of omitting critical viewpoints that could arise if only a portion of the population were studied.

### *3.3. Sampling technique*

Sampling technique refers to the method used to select respondents from a population [27]. This study employs a *total enumeration (census) sampling technique*, which involves including every member of the population who meets the inclusion criteria. Census sampling is particularly suitable when the population is small, accessible, and directly relevant to the research problem [28].

Total enumeration eliminates sampling error and ensures full representation of the population's perspectives. This is especially important in studies of digital security, where responsibilities and exposure to risks may vary across staff categories. Given the population size of 125 staff members, total enumeration is both practical and methodologically sound, enhancing the credibility and applicability of the findings.

### *3.4. Instrument for data collection*

The primary instrument for data collection in this study is a structured questionnaire developed by the researcher. Questionnaires are effective tools for collecting data on attitudes, beliefs, perceptions, and experiences that cannot be directly observed [15]. They also allow for efficient data collection from a large number of respondents within a limited time frame and ensure uniformity of responses, facilitating quantitative analysis [29], [30].

The instrument, titled *Staff Questionnaire on Risk Management and Security of Digital Collections (SQRMSDC)*, was designed to elicit information on awareness of risk management, types of risks affecting digital collections, existing security policies and measures, staff involvement, capacity and training, and strategies for improving digital security [38].

#### *3.4.1. Description of the instrument*

The questionnaire is divided into two main sections. Section A captures demographic information such as gender, academic qualification, years of service, and designation. Section B contains 16 analytical items structured under four thematic areas aligned with the study objectives. These items include five-point Likert-scale questions, closed-ended questions, and a limited number of open-ended questions.

Open-ended questions allow respondents to express their views and experiences in detail, while closed-ended questions provide standardized responses suitable for statistical analysis [22]. The integration of multiple question formats ensures balanced coverage of attitudinal and practical dimensions of risk management and digital security [30].

#### *3.4.2. Procedure for instrument development*

The development of the questionnaire followed a systematic process to ensure clarity, relevance, and validity. First, the study objectives were analyzed to identify key variables. Second, an extensive literature review was conducted to inform item construction [31], [32], [7]. A draft questionnaire was then developed and reviewed by experts in library and information science and research measurement.

Expert review ensured that the instrument was contextually appropriate, clearly worded, and capable of eliciting meaningful responses. Feedback from this process informed revisions prior to pilot testing.

### *3.5. Validity and reliability of the instrument*

#### *3.5.1. Validity*

Validity refers to the extent to which an instrument measures what it is intended to measure [23], [24]. Both content and face validity were established. Content validity was ensured by grounding questionnaire items in relevant literature and aligning them with the research objectives. Face validity involved expert assessment of the instrument's clarity, relevance, and appropriateness [27].

A pilot study involving 10 respondents from an academic library outside the study population was conducted to test the instrument. Feedback from the pilot study informed refinements to improve clarity, structure, and flow.

#### *3.5.2. Reliability*

Reliability refers to the consistency with which an instrument measures a construct under similar conditions [15]. Reliability was assessed through pilot testing and analysis using Cronbach's Alpha, a widely accepted measure of internal consistency [32]. A coefficient of 0.70 or higher was considered acceptable, indicating adequate reliability.

Items contributing to low reliability were revised or removed to improve internal consistency, ensuring that the final instrument was dependable and robust.

### *3.6. Procedure for data collection*

Data collection commenced after obtaining formal approval from the University of Jos Library management. Questionnaires were distributed personally to respondents during working hours using a self-administered approach, which minimized non-response and allowed clarification of instructions where necessary [9]. Participation was voluntary, and confidentiality was assured in line with ethical research standards [33], [37].

Respondents were given one to two weeks to complete the questionnaire, with follow-up reminders provided to enhance response rates. Completed questionnaires were collected securely to ensure data integrity.

### *3.7. Method of data analysis*

Data were analyzed using the Statistical Package for the Social Sciences (SPSS), version 26. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were used to summarize demographic data and responses to Likert-scale items [9]. Inferential statistics, such as chi-square tests and independent samples t-tests, were employed to examine relationships among variables.

All inferential analyses were conducted at the 0.05 level of significance. Open-ended responses were analyzed thematically to complement quantitative findings and provide contextual depth.

## 4. Results

This section presents findings from 67 valid responses (53.6% response rate) obtained from professional and paraprofessional staff of the University of Jos Library. Results are organized around respondent demographics, availability and effectiveness of risk-management practices, adoption of security technologies, and staff capacity for managing digital collections.

### *4.1. Demographic characteristics of respondents*

Table 1 summarizes respondent demographics. Males constituted 58.2% while females were 41.8%. In terms of designation, 52.2% were library staff, 17.9% were academic librarians, and 29.9% were para-professional staff. All respondents reported six years or more working experience, supporting the reliability of responses on institutional practices.

Table 1: Demographic characteristics of respondents ($n = 67$)

| S/N | Variable | Category | Number | Percentage (%) |
|---|---|---|---|---|
| 1 | Gender | Male | 39 | 58.2 |
| | | Female | 28 | 41.8 |
| 2 | Position | Library Staff | 35 | 52.2 |
| | | Academic Librarian | 12 | 17.9 |
| | | Para-professional | 20 | 29.9 |
| 3 | Years in library | 6 years and above | 67 | 100.0 |

Table 2: Availability of risk-management practices (multiple responses allowed; $n = 67$)

| S/N | Practice | Yes | Yes (%) | No | No (%) |
|---|---|---|---|---|---|
| 1 | Fire-safety alarms | 56 | 83.6 | 11 | 16.4 |
| 2 | Access control | 52 | 77.6 | 15 | 22.4 |
| 3 | Regular data backup | 44 | 65.7 | 23 | 34.3 |
| 4 | User authentication | 43 | 64.2 | 24 | 35.8 |
| 5 | Antivirus/malware protection | 38 | 56.7 | 29 | 43.3 |
| 6 | Disaster-recovery plan | 35 | 52.2 | 32 | 47.8 |
| 7 | Environmental control | 38 | 56.7 | 29 | 43.3 |
| 8 | Security-awareness programme | 32 | 47.8 | 35 | 52.2 |
| 9 | Incident-response teams | 5 | 7.5 | 62 | 92.5 |

### *4.2. Availability of risk management practices*

Availability of risk-management practices is presented in Table 2. Fire-safety alarms (83.6%) and access control (77.6%) were widely reported. Regular data backup (65.7%) and user authentication (64.2%) were moderately implemented. However, incident-response teams were largely absent (7.5%), indicating weak readiness for coordinated response to digital security events.

### *4.3. Risk assessment frequency and policy awareness*

Table 3 shows that risk assessment was not consistently performed: 37.3% reported it was rarely or never conducted. Policy awareness was mixed; while 50.8% were aware/very aware, 29.8% were unaware/very unaware, suggesting a need for stronger policy communication and enforcement.

Table 3: Frequency of risk assessment and awareness of written risk-management policy ($n = 67$)

| Frequency of risk assessment | Number | Percentage (%) |
|---|---|---|
| Always | 8 | 11.9 |
| Often | 12 | 17.9 |
| Sometimes | 22 | 32.8 |
| Rarely | 16 | 23.9 |
| Never | 9 | 13.4 |
| **Awareness of written policy** | | |
| Very aware | 15 | 22.4 |
| Aware | 19 | 28.4 |
| Neutral | 13 | 19.4 |
| Unaware | 12 | 17.9 |
| Very unaware | 8 | 11.9 |

### *4.4. Security measures for library resources*

Table 4 indicates a strong emphasis on physical surveillance (CCTV: 100.0%) and password-based controls (70.1%). Conversely, advanced digital safeguards such as intrusion detection (7.5%) and encryption/watermarking (11.9%) were limited, increasing exposure to cyber threats targeting digital repositories.

### *4.5. Perceived effectiveness of risk-management measures*

As shown in Table 5, only 9.0% rated the measures as very effective. The most common view was moderate effectiveness (35.8%), reflecting that existing controls provide baseline protection but do not fully address evolving digital security risks.

### *4.6. Security incidents and adequacy of measures*

Table 6 shows that 44.8% of respondents reported experiencing incidents in past years. Perceptions of adequacy were mixed: 47.7% rated measures adequate/very adequate, while 35.8% rated them inadequate/very inadequate, indicating a need for strengthened safeguards and clearer operational readiness.

### *4.7. Technologies adopted for risk mitigation*

Table 7 indicates notable adoption of integrated library systems (80.6%), bar-code systems (83.6%), and firewalls/network security (76.1%). Cloud storage was also reported (68.7%). However, biometric scanners were absent and digital asset management was below 50%, suggesting incomplete modernization of access control and digital-asset governance.

### *4.8. Level of digitization and expansion plans*

As shown in Table 8, digitization was mostly partial (52.2%) or minimal (23.9%), with no reports of complete digitization. Nevertheless, 74.6% indicated that expansion plans were likely/very likely, emphasizing the urgency of strengthening risk-management capacity to support future digital growth.

Table 4: Security measures for library resources (multiple responses allowed; $n = 67$)

| S/N | Measure | Present | Present (%) | Not present | Not present (%) |
|---|---|---|---|---|---|
| 1 | Alarms | 15 | 22.4 | 52 | 77.6 |
| 2 | CCTV cameras | 67 | 100.0 | 0 | 0.0 |
| 3 | Intrusion detection system | 5 | 7.5 | 62 | 92.5 |
| 4 | Password-based access control | 47 | 70.1 | 20 | 29.9 |
| 5 | Encryption and watermarking | 8 | 11.9 | 59 | 88.1 |
| 6 | Others | 0 | 0.0 | 67 | 100.0 |

Table 5: Perceived effectiveness of risk-management measures (0–10 scale; $n = 67$)

| S/N | Score band | Number | Percentage (%) |
|---|---|---|---|
| 1 | 9–10 (Very effective) | 6 | 9.0 |
| 2 | 7–8 (Effective) | 20 | 29.9 |
| 3 | 5–6 (Moderate) | 24 | 35.8 |
| 4 | 3–4 (Low) | 12 | 17.9 |
| 5 | 0–2 (Not effective) | 5 | 7.5 |

Table 6: Incident records and perceived adequacy of security measures ($n = 67$)

| Incidents in past years | Number | Percentage (%) |
|---|---|---|
| Yes | 30 | 44.8 |
| No | 37 | 55.2 |
| **Adequacy of measures** | | |
| Very adequate | 10 | 14.9 |
| Adequate | 22 | 32.8 |
| Neutral | 11 | 16.4 |
| Inadequate | 16 | 23.9 |
| Very inadequate | 8 | 11.9 |

### *4.9. Staff training, skills, and capacity*

Table 9 shows that training was mostly occasional (44.8%) or rare/never (38.8%). Technical skill familiarity was largely moderate (40.3%), and perceived capacity to meet needs was mostly sometimes (35.8%) or rarely (23.9%). These patterns suggest that technology availability is not matched by consistent skills development, which is necessary for sustainable digital security.

### *4.10. Training needs for effective risk management*

Table 10 identifies the most requested training areas: digital literacy/ICT (76.1%), e-resources and database management (68.7%), and integrated library management (64.2%). Cyber-threat intelligence (47.8%) also emerged as a substantial need, consistent with increasing exposure of academic libraries to cyber risks.

## 5. Discussion

This discussion interprets the findings of the study on risk management and security of digital collections in the University of Jos Library, drawing on responses from 67 experienced staff members representing professional and paraprofessional categories. The analysis focuses on four core areas: existing risk management practices, effectiveness of security measures, technologies adopted for risk mitigation, and staff capacity building and training. While the library demonstrates strengths in physical and basic technological safeguards, significant gaps in procedural consistency, policy awareness, advanced digital security, and staff training weaken its overall risk management framework.

The findings indicate a strong institutional emphasis on physical security controls. High adoption rates of fire-safety alarms, access control mechanisms, and universal deployment of CCTV cameras (Tables 2 and 4) suggest that the library prioritizes visible and traditional safeguards against threats such as theft and fire outbreaks. This pattern aligns with observations that academic libraries in developing contexts often focus on affordable and tangible security measures due to financial and infrastructural constraints. However, physical security alone is insufficient in environments increasingly dependent on digital technologies.

Significant weaknesses are evident in procedural and organizational aspects of risk management. The near absence of incident-response teams and limited implementation of security-awareness programmes (Table 2) indicate inadequate preparedness for handling emergencies and security breaches. Moreover, irregular risk assessment practices and limited awareness of written risk management policies (Table 3) suggest weak governance structures. This imbalance implies that while physical assets may be protected, the library lacks systematic planning and staff coordination necessary for effective risk prevention and response. Similar studies have cautioned that over-reliance on physical controls without structured procedures increases exposure to internal risks such as staff negligence and operational errors [34]–[36].

Perceptions of effectiveness further underscore these shortcomings. Although a majority of staff rated existing measures as moderately effective or effective, a substantial proportion reported incidents of damage or loss in previous years and rated security measures as inadequate (Tables 5 and 6). This suggests that existing safeguards are insufficiently robust to prevent or mitigate incidents consistently. Prior research has similarly noted that security systems

Table 7: Adoption of technologies for risk mitigation (multiple responses allowed; $n = 67$)

| S/N | Technology | Present | Present (%) | Not present | Not present (%) |
|---|---|---|---|---|---|
| 1 | Integrated library system (ILS) | 54 | 80.6 | 13 | 19.4 |
| 2 | Institutional repository software | 40 | 59.7 | 27 | 40.3 |
| 3 | Digital asset management | 32 | 47.8 | 35 | 52.2 |
| 4 | Cloud storage | 46 | 68.7 | 21 | 31.3 |
| 5 | Biometric scanners | 0 | 0.0 | 67 | 100.0 |
| 6 | Firewalls and network security | 51 | 76.1 | 16 | 23.9 |
| 7 | Bar-code systems | 56 | 83.6 | 11 | 16.4 |
| 8 | Others | 0 | 0.0 | 67 | 100.0 |

Table 8: Level of digitization and expansion plans ($n = 67$)

| Digitization level | Number | Percentage (%) |
|---|---|---|
| Fully digitized | 0 | 0.0 |
| Largely digitized | 11 | 16.4 |
| Partially digitized | 35 | 52.2 |
| Minimally digitized | 16 | 23.9 |
| Not digitized | 5 | 7.5 |
| **Expansion plans** | | |
| Very likely | 42 | 62.7 |
| Likely | 8 | 11.9 |
| Neutral | 11 | 16.4 |
| Unlikely | 4 | 6.0 |
| Very unlikely | 2 | 3.0 |

Table 9: Staff training frequency, technical skill familiarity, and capacity to meet needs ($n = 67$)

| Training frequency | Number | Percentage (%) |
|---|---|---|
| Regularly | 11 | 16.4 |
| Occasionally | 30 | 44.8 |
| Rarely | 19 | 28.4 |
| Never | 7 | 10.4 |
| **Technical skill familiarity** | | |
| Very high | 8 | 11.9 |
| High | 22 | 32.8 |
| Moderate | 27 | 40.3 |
| Low | 10 | 14.9 |
| **Capacity to meet needs** | | |
| Always | 5 | 7.5 |
| Often | 14 | 20.9 |
| Sometimes | 24 | 35.8 |
| Rarely | 16 | 23.9 |
| Never | 8 | 11.9 |

in academic libraries often suffer from inadequate maintenance, monitoring, and evaluation, which diminishes their long-term effectiveness [36].

The low adoption of advanced digital security technologies exacerbates these challenges. Intrusion detection systems, encryption, and watermarking are minimally implemented (Table 4), exposing digital collections to cyber threats such as unauthorized access, data breaches, and ransomware attacks. The absence of structured incident-response mechanisms further limits the library's ability to recover from such incidents. Studies on digital library security emphasize that preventive controls must be complemented by response and recovery strategies to ensure resilience [8], [33] .

Technology adoption patterns reveal a reliance on barcode systems, integrated library systems, and basic network security tools (Table 7). While these technologies support routine operations and resource tracking, the absence of biometric systems and limited use of digital asset management platforms indicate underinvestment in advanced access control and content protection. This finding mirrors reports that many African academic libraries adopt technologies that support daily operations but lag behind in deploying sophisticated security solutions due to cost and skill limitations [9].

The level of digitization presents additional implications. With most collections partially digitised and strong intentions for further expansion (Table 8), the library is transitioning toward a more digitally dependent environment. Partial digitization increases exposure to both physical and digital risks, especially when advanced security measures are not concurrently strengthened. Without adequate safeguards, expanded digitization may amplify vulnerabilities rather than enhance access and preservation [22].

Staff capacity building emerges as a critical concern. Training is irregular, technical skill familiarity is largely moderate, and many staff members report limited capacity to meet digital security needs (Table 9). High demand for training in digital literacy, e-resource management, and integrated library systems (Table 10) reflects awareness of existing skill gaps. However, the relatively low prioritization of cyber-threat intelligence training suggests limited understanding of emerging digital risks. Previous studies have demonstrated that inadequate and irregular training undermines staff readiness to manage modern digital

Table 10: Training areas required (multiple responses allowed; $n = 67$)

| S/N | Training area needed | Needed | Needed (%) | Not needed | Not needed (%) |
|---|---|---|---|---|---|
| 1 | Digital literacy and ICT | 51 | 76.1 | 16 | 23.9 |
| 2 | Integrated library management | 43 | 64.2 | 24 | 35.8 |
| 3 | E-resources and database management | 46 | 68.7 | 21 | 31.3 |
| 4 | Cyber-threat intelligence | 32 | 47.8 | 35 | 52.2 |
| 5 | Information literacy programmes | 35 | 52.2 | 32 | 47.8 |
| 6 | Leadership and supervisory skills | 38 | 56.7 | 29 | 43.3 |

threats effectively [37], [17].

Overall, the University of Jos Library demonstrates commendable efforts in deploying physical security measures and basic technologies. However, deficiencies in governance, procedural consistency, advanced digital safeguards, and staff training expose the library to avoidable risks. These findings reinforce the need for a holistic risk management approach that integrates regular risk assessments, effective policy communication, investment in advanced security technologies, and sustained capacity building. Such a multifaceted strategy is essential to safeguarding digital collections and supporting the library's ongoing digitization initiatives.

### *5.1. Methodological scope and research implications*

While the findings provide important insights into risk management and security of digital collections at the University of Jos Library, they should be interpreted within certain methodological boundaries. The study was conducted within a single academic institution, which limits the extent to which the findings can be generalized to libraries operating under different administrative structures, funding models, or technological capacities. In addition, reliance on self-reported questionnaire data introduces the possibility of response bias, particularly on sensitive issues related to security practices and institutional preparedness. Furthermore, the analysis did not explicitly account for broader external constraints such as funding availability, national policy environments, or infrastructural limitations, all of which may influence the adoption of advanced risk management measures.

These limitations, however, point directly to important directions for future research. Comparative studies across multiple academic libraries would enhance generalization and enable benchmarking of best practices. Further investigations examining the impact of advanced technological interventions—such as biometric authentication systems, automated risk assessment tools, and fully digitized record-keeping—would provide empirical evidence on their effectiveness in strengthening library security frameworks. Longitudinal studies assessing the effects of sustained staff training programmes on risk reduction and policy compliance are also recommended. Addressing these areas will contribute to a deeper and more comprehensive understanding of institutional risk management in academic libraries.

## 6. Conclusion

This study evaluated risk management practices at the University of Jos Library, with specific focus on existing safeguards, their effectiveness, technologies used for risk mitigation, and staff capacity for securing digital collections. The findings reveal that the library has established a foundational level of physical and basic technological safeguards; however, systemic weaknesses in procedural governance, advanced security infrastructure, and human capacity significantly constrain the overall effectiveness of its risk management framework.

The most consistently implemented measures include fire-safety alarms (84.0%), access control mechanisms (78.4%), and CCTV surveillance (100.0%), reflecting a strong institutional emphasis on protecting physical assets and deterring unauthorized access. Moderate adoption of data backup systems (65.6%) and user authentication mechanisms (64.0%) indicates growing awareness of digital risks. Nonetheless, advanced security measures remain largely absent, with only 7.2% of respondents reporting the presence of intrusion detection systems and 12.0% indicating the use of encryption or watermarking technologies.

Procedural mechanisms were found to be notably weak. Only 8.0% of respondents confirmed the existence of incident-response teams, while risk assessments are conducted inconsistently, with just 12.0% indicating that they occur regularly. Policy visibility is similarly limited, as only 50.4% of staff reported awareness of written risk management policies. These deficiencies suggest that risk management within the library is predominantly reactive, with limited institutional preparedness for emerging digital and operational threats. Although a majority of respondents rated existing measures as moderately effective (36.0%) or effective (30.4%), a substantial proportion reported previous incidents of damage or loss (44.0%) and considered current safeguards to be inadequate (36.0%). This disparity underscores the insufficiency of existing controls, particularly within an increasingly digital environment.

Technological adoption is strongest in bar-code systems (84.0%), Integrated Library Systems (80.0%), and network firewalls (76.0%). However, the absence of advanced tools such as biometric authentication systems and the low uptake of digital asset management platforms indicate limited readiness for securing expanding digital collections. With 52.0% of resources only partially digitized and 75.2% of respondents anticipating further digitization, the likelihood of increased vulnerabilities is high unless security measures are correspondingly strengthened.

Capacity building remains a critical constraint. Staff training is largely occasional (44.0%) or rare (28.0%), while technical skills are predominantly moderate (40.0%), and only 28.0% of respondents believe that institutional capacity consistently meets digital security needs. The high demand for training in digital literacy (76.0%), e-resource management (68.0%), and integrated library systems (64.0%) highlights the urgency of strengthening staff competence in alignment with the library's digitization trajectory.

Overall, the University of Jos Library demonstrates commendable baseline security practices. However, deficiencies in procedural consistency, advanced technological safeguards, and staff preparedness expose the institution to avoidable risks. A coordinated and integrated strategy encompassing policy enforcement, technological modernization, and sustained professional development is essential to achieving resilient and sustainable protection of both physical and digital library assets.

## 7. Recommendations

Based on the findings of this study, the following recommendations are proposed to enhance risk management practices at the University of Jos Library:

1. Establish a robust incident-response framework, including dedicated response teams, to improve preparedness and minimize the impact of security incidents, addressing the current low adoption rate (8.0%).
2. Institutionalize regular risk assessments with a clearly defined schedule to proactively identify and mitigate threats, given that 70.4% of respondents reported assessments as occurring sometimes, rarely, or never.
3. Develop, document, and widely disseminate comprehensive written risk management policies to improve staff awareness, compliance, and accountability, as only 50.4% of staff are currently aware of such policies.
4. Invest in advanced security technologies, including biometric authentication systems, intrusion detection mechanisms (currently 7.2% adoption), and encryption or watermarking solutions (12.0%), to strengthen protection of digital and sensitive resources.
5. Implement continuous and targeted staff training programmes in digital literacy (76.0% demand), e-resource management (68.0%), integrated library systems (64.0%), and cybersecurity to address skill gaps and enhance institutional capacity to meet evolving security demands.

## Declarations and Ethical Statements

***Conflict of Interest:*** The authors declare that there is no conflict of interest.

***Funding Statement:*** The authors declare that no specific funding was received for this research.

***Artificial Intelligence usage Statement:*** During the preparation of this work, the author used Grammarly to assist with grammatical corrections. After using this tool, the author reviewed and edited the content as needed and take full responsibility for the content of the published article.

***Availability of Data and Materials:*** Primary data will be made available upon reasonable request to the corresponding author, subject to privacy constraints.

***Publisher's Note:*** The publisher of this article, Krrish Scientific Publications, remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

## References

[1] Abioye A, Adeowu O. Security risks management in selected academic libraries in Osun State, Nigeria. *The Information Manager*. 2013;13(1–2):1–9. Available from: https://www.gatewayinfojournal.org/index.php/gij/article/download/35/32/39

[2] Mabawonku OT, Madukoma E. Information security awareness and information security compliance in university libraries in South-West, Nigeria. *Library Philosophy and Practice*. 2022;(7215). Available from: https://digitalcommons.unl.edu/libphilprac/7215

[3] Anday A, Francese E, Huurdeman HC, Yılmaz M, Zengenene D. Information security issues in a digital library environment: A literature review. *Bilgi Dünyası*. 2012 Apr 30;13(1):117-37. Available from:https://doi.org/10.15612/BD.2012.171

[4] Patra S, Sahoo J. A literature review on digitization in libraries and digital libraries. *Preservation, Digital Technology & Culture*.2022 Apr 26;51(1):17-26. Available from: https://doi.org/10.1515/pdtc-2021-0023

[5] Umar L. Adoption of risk management strategies in information resources and services provision in university libraries in northern states of Nigeria. *Information Impact: Journal of Information and Knowledge Management*. 2016. Available from: https://www.academia.edu/125473849/Adoption_of_risk_management_strategies_in_information_resources_and_services_provision_in_university_libraries_in_northern_states_of_Nigeria

[6] Shenkir WG, Barton TL, Walker PL. Enterprise risk management: Lessons from the field. In: *Enterprise risk management*. Hoboken (NJ): John Wiley & Sons; 2009. p. 441–463. Available from: https://doi.org/10.1002/9781118267080.ch24

[7] Rodriguez JC, Zhang B. Authentication and access management of electronic resources. In *IGI Global eBooks*. 2008. p. 250–74. Available from: https://doi.org/10.4018/978-1-59904-891-8.ch014

[8] Lawrence GW, Kehoe WR, Rieger OY, Walters WH, Kenney AR. Risk Management of Digital Information: A File Format Investigation. *Council on Library and Information Resources*, 1755 Massachusetts Avenue, NW, Suite 500, Washington, DC 20036; 2000 Jun. Available from: https://eric.ed.gov/?id=ED449802

[9] Maidabino AA, Zainab AN. Collection security management in university libraries in Nigeria. *Malaysian Journal of Library and Information Science*. 2013;16(1):15–33. Available from: https://mjlis.um.edu.my/article/view/6675/4360

[10] Ike N. Knowledge sharing practices in academic libraries in Imo State, Nigeria. *DigitalCommons@University of Nebraska - Lincoln*. Available from: https://digitalcommons.unl.edu/libphilprac/7626/

[11] Anyaoku EN, Echedom AUN, Baro EE. Digital preservation practices in university libraries: An investigation of institutional repositories in Africa. *Digital Library Perspectives*. 2019;35(1):41–64. Available from: https://doi.org/10.1108/DLP-10-2017-0041

[12] Leijen D. *Computer security*. Utrecht (Netherlands): University of Utrecht; 2001. Available from: https://www.uu.nl/en/organisation/information-and-technology-services-its/what-we-do/information-security

[13] Toyese OT. Digital threats to libraries and their impact on sustainable development goals (SDGs). Zenodo; 2024 Nov. Available from: `https://doi.org/10.5281/zenodo.14202358`

[14] Anyim WO, Okereke W. Internal Control and Risk Management System in University Libraries: Applications, Techniques and Limitations. *Library Philosophy and Practice (e-journal)*. 2020;(4167). Available from: `https://digitalcommons.unl.edu/libphilprac/4167`.

[15] Iwara FU. Security abuse of library materials and prevention in academic libraries: A case study of Kenneth Dike Library, University of Ibadan, Nigeria. *Library Philosophy and Practice*. 2007:118–129. Available from: `https://journals.ui.edu.ng/index.php/uijlis/article/view/849`

[16] Anyaobi G, Akpoma O. Abuse of library materials in academic libraries: A case study of Delta State Polytechnic Library, Ogwashi-Uku, Nigeria. *Journal of Research in Education and Society*. 2012 Apr;3(1):54-8. Available from: `https://api.semanticscholar.org/CorpusID:110320478`

[17] Nakiyingi RL. Strengthening Cybersecurity in Nigerian Libraries: Challenges, Mitigation Strategies, and Future Trends. *Res Output J Biol Appl Sci*. 2024;3(2):23-27. Available from: `https://rojournals.org/strengthening-cybersecurity-in-nigerian-libraries-challenges-mitigation-strategies-and-future-trends/`

[18] Musa H, Yelwa AS. Data Privacy and Security Challenges in Digital Libraries of Tertiary Institutions in Zamfara State. FUGUS International Journal of Library and Information Science. 2025 Nov 10;2(2):79-89. Available from: `https://doi.org/10.57233/fijlis.v2i2.08`

[19] Gladness K, Ibrahim Z. Investigating Ineffectiveness of Electronic Security Systems in Safeguarding Library Materials at Mzumbe University Library: Challenge Of Using Electronic Security Systems In Academic Libraries. *International Journal of Librarianship*. 2025 Mar 31;10(1):13-35. Available from: `https://journal.calaijol.org/index.php/ijol/article/view/438`

[20] Alhaji YM, Awwal NM, Umar DAD. Digital Preservation Strategies for Long-Time Access to Information in Federal University Library Gashua, Yobe State, Nigeria. *Al-Hikmah Journal of Arts & Social Sciences Education*. 2023;5(2). Available from: `https://alhikmahuniversity.edu.ng/AJASSE/index.php/journal/article/download/122/134`.

[21] Okocha F. Digital libraries in Africa: Challenges and opportunities. *Library Philosophy and Practice*. 2022. Available from: `https://digitalcommons.unl.edu/libphilprac/7288/`

[22] Yakubu H, Noorhidawati A, Kiran K. Sustainability of digital collections for Nigerian academic libraries: An exploration of conception, indicators for fulfillment and accrued benefits. Malays J Libr Inf Sci. 2022;27(1):73-91. Available from: `https://doi.org/10.22452/mjlis.vol27no1.5`

[23] Richards K, Ross S, Seedhouse P. Research methods for applied language studies: An advanced resource book for students. Londres: Routledge; 2012. Available from: `https://api.semanticscholar.org/CorpusID:60779662`

[24] Creswell JW, Creswell JD. Research design: Qualitative, quantitative, and mixed methods approaches. *Sage publications*; 2017 Dec 12. Available from: `https://uk.sagepub.com/en-gb/eur/research-design/book270550`

[25] Park J-ran, Tosaka Y. Metadata Creation Practices in Digital Repositories and Collections: Schemata, Selection Criteria, and Interoperability. ITAL [Internet]. 2010 Sep 1 [cited 2026 Feb 8];29(3):104-116. Available from: `https://ital.corejournals.org/index.php/ital/article/view/3136`

[26] Eze J, Uzoigwe CU. The place of academic libraries in Nigerian University Education: contributing to the 'Education for All' initiative. Int J Libr Inf Sci. 2013;5:432-438. Available from: `https://academicjournals.org/journal/IJLIS/article-abstract/1B1730041571`

[27] Bolarinwa O. Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. *Nigerian Postgraduate Medical Journal*. 2015 Jan 1;22(4):195. Available from: Available from: `https://doi.org/10.4103/1117-1936.173959`

[28] Etikan I. Sampling and sampling methods. *Biometrics & Biostatistics International Journal*. 2020;8(1):1–3. Available from: `https://doi.org/10.15406/bbij.2017.05.00149`

[29] Joint N. Risk assessment and copyright in digital libraries. *Library Review*. 2006;55(9):545-548. Available from: `https://doi.org/10.1108/00242530610706743`

[30] Musa S. Digital Preservation in Nigeria Universities Libraries: A Comparison Between University of Nigeria Nsukka and Ahmadu Bello University Zaria. 2016. Available from: `https://www.academia.edu/108891965/Digital_Preservation_In_Nigeria_Universities_Libraries_A_Comparison_Between_University_Of_Nigeria_Nsukka_And_Ahmadu_Bello_University_Zaria`

[31] Magsi I, Shaheen N, Channar WA, Ali M, Lakho Z, Ahmed A. Cyber-security challenges in digital libraries. *RJSP*. 2025;3(1):344–350. Available from: `https://socialworksreview.com/index.php/Journal/article/view/102`.

[32] Sirhan AA, Abdrabbo KM, Tawalbeh SAAA, Ahmed MH, Helalat MA. Digital rights management (DRM) in libraries of public universities in Jordan. *Library Management*. 2019 Sep 25;40(8/9):496–502. Available from: `https://doi.org/10.1108/lm-05-2018-0044`

[33] Saunders M, Lewis P, Thornhill A. Research methods for business students. *Qualitative Market Research an International Journal*. 2000 Dec 1;3(4):215–8. Available from: `https://doi.org/10.1108/qmr.2000.3.4.215.2`

[34] Smith M. Exploring Variety in Digital Collections and the Implications for Digital Preservation. *Library Trends*. Urbana; 2005 Summer;54(1):6-15. Available from: `https://dspace.mit.edu/handle/1721.1/30592`

[35] Oguedoihu JC, Adinchezor IP. Library and Information Services and Security Challenges in Two Selected Academic Libraries in Southeast Nigeria. *Ghana Library Journal*. 2022;27(2):211–220. Available from: `https://doi.org/10.4314/glj.v27i2.7`

[36] Sunday OO, Nwoke OM, Ajibola RR, Ogundana AA, Giwa AO, Olaseigbe YF, Ogunojemite AT. Adoption of Electronic Security Systems in Three Academic Libraries in Southwestern Nigeria. *Jewel Journal of Librarianship*. 2025;20(2). Available from: `https://www.jeweljournals.com/admin/published/21721326808.pdf`.

[37] Whong FM, Ezra SG. Academic librarians ICT competency and its effect on management of information resources in selected federal Nigerian academic libraries. *Journal of Applied Information Science and Technology*. 2016;9(1):209-18. Available from: `https://www.jaistonline.org/vol9_no1_Whong_Ezra.pdf`

[38] [Online Available]: University of Jos Library. Available from: `https://www.unijos.edu.ng/library`