Studi Akuntansi, Keuangan, dan Manajemen (SAKMAN)
ISSN 2798-0251, Vol 6, No 1, 2026, 441-458 https://doi.org/10.35912/sakman.v6i1.6568

A Process-Based Vulnerability Assessment Model for Accounting Data Security in Microfinance Institutions

Anita Wijayanti[1*], Massila Kamalrudin[2], Kartika Hendra Titisari[3]
Universitas Islam Batik Surakarta, Surakarta, Indonesia[1,3]
University Technology Malaysia, Melaka, Malaysia[2]
itax_solo@yahoo.com[1*], massila@gmail.com[2], kartikatitisari@gmail.com[3]

Article History
Received on 28 April 2026
1st Revised on 29 April 2026
2nd Revised on 03 June 2026
3rd Revised on 11 June 2026
4th Revised on 23 June 2026
Accepted on 08 July 2026

Abstract
Purpose: This study aims to examine how accounting data vulnerabilities emerge and how vulnerability assessment is practiced in microfinance institutions, as well as to develop a context-based vulnerability assessment model.
Methodology: This research was conducted in Surakarta, Indonesia, involving Rural Banks, Islamic Rural Banks, and savings and loan cooperatives. A multi-case qualitative approach was used through semi-structured interviews, focus group discussions, and document analysis. Data were analyzed using thematic analysis to identify patterns of vulnerability and assessment practices.
Results: The findings show that accounting data vulnerabilities are influenced by technical limitations, human resource constraints, weak governance, and short-term managerial decisions. Vulnerability assessment practices are mostly reactive, informal, and not well integrated into organizational processes.
Conclusions: The study proposes a process-based vulnerability assessment model consisting of four stages: capacity-based identification, vulnerability evaluation, managerial decision integration, and organizational learning, positioning vulnerability assessment as an iterative socio-technical process.
Limitations: The study is limited to a small number of cases within a single regional context and mainly reflects internal organizational perspectives.
Contributions: This study contributes to accounting information systems and cybersecurity research by providing a practical and context-sensitive framework for microfinance institutions, offering insights for managers, regulators, and policymakers to strengthen accounting data security and organizational resilience.

Keywords: *Accounting Data Security, Microfinance Institutions, Socio-Technical Approach, Vulnerability Assessment*

How to Cite: Wijayanti, A., Kamalrudin, M., Titisari, K. H., (2026). A Process-Based Vulnerability Assessment Model for Accounting Data Security in Microfinance Institutions. *Studi Akuntansi, Keuangan, dan Manajemen*, 6(1), 441-458.

1. Introduction

The acceleration of digitalization in the global financial sector has fundamentally transformed how organizations manage, store, and utilize financial data (Offiong, Szopik-Depczyńska, Cheba, & Ioppolo, 2024; Waliullah et al., 2025). The digitalization of accounting systems, the adoption of cloud computing, and the integration of cross-functional information systems have enhanced the efficiency and accuracy of financial reporting (Giessmann & Legner, 2013; Gou & Deng, 2023; Wijayanti, Mohamed, & Daud, 2024). At the same time, these developments have expanded the attack surface of accounting data, increasing exposure to cyber threats such as hacking, data breaches, ransomware, and insider misuse (Adejumo & Ogburie, 2025; Nguyen, Nguyen, Pham, Nguyen, & Vu, 2024; Waliullah et al., 2025). International reports consistently identify the financial sector as a primary target of global

cyberattacks due to the high economic value and sensitivity of the data it processes (Neri, Niccolini, & Rosario, 2022; Nurwanah, 2024).

Across countries, incidents involving accounting and financial data breaches are no longer confined to large financial institutions but increasingly affect small- and medium-sized entities, including Microfinance Institutions (MFIs) (Calvo-Manzano et al., 2025; Damayanti, Hamidah, & Titisari, 2026; El-Hajj & Mirza, 2024; Neri et al., 2022). Limited technological investment, insufficient information security expertise, and reliance on relatively simple digital systems often render MFIs more vulnerable to cyber threats (Calvo-Manzano et al., 2025; Neri et al., 2022; Šafár, Pekarčik, Morawiec, Rutecka, & Wieczorek-Kosmala, 2025). These vulnerabilities raise serious concerns, as accounting data breaches not only generate direct financial losses but may also undermine financial system stability and public trust (Morshed & Khrais, 2025; Nurwanah, 2024; Roup & Effendy, 2025). Similar patterns are emerging in Indonesia, where recent cases of data leakage and cyber incidents indicate that information security risks have extended beyond large corporations to smaller institutions, including MFIs (Calvo-Manzano et al., 2025; El-Hajj & Mirza, 2024; Neri et al., 2022; Šafár et al., 2025). In this context, accounting data security is critical, as such data reflects institutional financial conditions, underpins managerial decision-making, and is directly linked to regulatory compliance and customer protection (Chotia, Khoualdi, Broccardo, & Yaqub, 2025; Lwesya & Mwakalobo, 2023; Morshed & Khrais, 2025; Nurwanah, 2024). This issue is particularly relevant in Indonesia, where many microfinance institutions are undergoing rapid digitalization without proportional improvements in data security governance (Andromeda, Wahyuni, Tubastuvi, & Santoso, 2026).

For microfinance institutions such as Rural Banks, Islamic Rural Banks, and Savings and Loan Cooperatives, accounting data plays an indispensable strategic role (Nurwanah, 2024; Offiong et al., 2024; Pattnaik, Ray, & Hassan, 2024; Wijayanti et al., 2024). Beyond serving internal control and financial reporting functions, accounting data constitutes the foundation of customer trust and institutional legitimacy in the eyes of regulators (Roup & Effendy, 2025). Consequently, data breaches or misuse may result in severe consequences, including financial losses, legal sanctions, and reputational damage that is difficult to restore. To address escalating risks, various information system security approaches have been developed, among which vulnerability assessment has gained prominence (Bennouk et al., 2024; Roup & Effendy, 2025; Waweru, Karume, & Kibet, 2024). Vulnerability assessment refers to a systematic process of identifying, analyzing, and evaluating weaknesses within information systems that could be exploited by unauthorized actors (Gupta, Mishra, & Behera, 2024). Globally, it has been widely adopted as a core component of information security governance, particularly in organizations with high dependence on digital systems (Bukari, Koomson, & Annim, 2024; Raju, 2023).

Despite the rapid growth of cybersecurity literature in the financial sector, empirical studies remain heavily concentrated on large institutions characterized by complex Information Technology (IT) infrastructures, dedicated security units, and substantial financial and human resources (Bennouk et al., 2024; Jiang, Oo, Meng, Lim, & Sikdar, 2025; Shimizu & Hashimoto, 2026; Zlati, Ionescu, & Antohi, 2022). In practice, however, real-world incidents, such as ransomware attacks that have disrupted the operations of numerous small and regional banks, demonstrate that cybersecurity risks for micro-scale institutions are not merely theoretical (Javaheri, Fahmideh, Chizari, Lalbakhsh, & Hur, 2024; Nguyen et al., 2024). Microfinance institutions exhibit distinct operational characteristics, including fragmented accounting systems, high dependence on third-party vendors, limited IT human capital, and weak formal governance structures (El-Hajj & Mirza, 2024; Waliullah et al., 2025). These features shape a vulnerability profile that differs substantially from that of large banks and calls for context-specific vulnerability assessment approaches (Isa, Praswati, & Zulaekah, 2024). Existing studies tend to emphasize technical aspects, such as network or application vulnerabilities, while paying insufficient attention to organizational dimensions, managerial involvement, employee security awareness, and cost-effective remediation mechanisms suitable for resource-constrained institutions (Mirtaheri, Pugliese, & Pascucci, 2025; Raju, 2023).

Although information system security has been widely studied, research that specifically links vulnerability assessment to accounting data security remains limited. Most prior studies have focused on general system security without addressing the distinctive characteristics of accounting data related to financial reporting reliability, internal control, and regulatory compliance. Moreover, studies that integrate accounting perspectives with a socio-technical approach, particularly in the context of microfinance institutions in Indonesia, are still scarce. Motivated by this gap, this study explores vulnerabilities in accounting data security by examining how microfinance institutions employ vulnerability assessment as a practical mechanism to evaluate and strengthen the protection of accounting data. This study offers three main contributions to the literature. First, it extends vulnerability and cybersecurity research by shifting the analytical focus from large financial institutions to microfinance institutions, which remain underrepresented despite their increasing digital exposure. Second, it conceptualizes vulnerability assessment as a socio-technical process by integrating technical weaknesses with organizational factors, managerial involvement, and human resource constraints that collectively shape accounting data security in microfinance institutions. Third, this study provides context-sensitive insights that support the development of feasible and cost-efficient vulnerability assessment practices tailored to resource-constrained microfinance institutions, thereby offering practical implications for regulators, managers, and policymakers in safeguarding accounting data integrity and enhancing institutional resilience.

2. Literature Review

2.1 Organizational Vulnerability in Accounting Systems

In organizational literature, vulnerability is conceptualized as a condition in which systems, processes, and resources contain weaknesses that may be exploited by internal or external threats, potentially disrupting operational continuity and the achievement of strategic objectives (Bennouk et al., 2024). Within accounting contexts, such vulnerabilities extend beyond technical deficiencies to include weaknesses in internal control structures, managerial oversight, and governance mechanisms that influence the reliability and integrity of accounting information. Organizational vulnerability is therefore embedded in managerial practices, decision-making routines, and institutional arrangements that shape how accounting risks are identified, prioritized, and managed. Weak coordination between accounting functions, limited segregation of duties, and informal control practices may amplify exposure to data manipulation, unauthorized access, and reporting errors. As a result, vulnerability in accounting systems reflects a socio-organizational condition rather than a purely technological problem.

2.2 Vulnerability Assessment as a Socio-Technical Process

Vulnerability assessment is defined as a systematic process for identifying levels of exposure, sensitivity, and adaptive capacity of a system in relation to both technical and non-technical threats (Jiang et al., 2025; Shimizu & Hashimoto, 2026). In accounting information systems, this process involves evaluating not only software and infrastructure weaknesses but also human behavior, control procedures, and managerial responses that influence data security and reporting reliability. This perspective represents a shift from security approaches centered on technical vulnerability scanning toward a more holistic and context-sensitive analytical framework. Within this framework, vulnerability assessment functions as a strategic tool for strengthening organizational resilience by linking technical safeguards with managerial decision-making and learning processes (Torkamani et al., 2025). Organizational vulnerability cannot be separated from social dynamics, power relations, and decision-making practices that determine how risks are interpreted and addressed. Accordingly, vulnerability assessment in accounting systems must be understood as a socio-technical process shaped by both technological configurations and organizational behavior (Shimizu & Hashimoto, 2026)

2.3 Vulnerability Assessment in Microfinance Institutions

Prior studies indicate that microfinance institutions face distinctive structural constraints, including limited financial resources, shortages of cybersecurity expertise, and low managerial awareness of digital and accounting data risks (El-Hajj & Mirza, 2024). These constraints directly affect the design and effectiveness of vulnerability assessment practices in microfinance settings (Lwesya & Mwakalobo, 2023). In addition, restricted computational capacity and limited operational resources often prevent microfinance institutions from adopting complex or standardized security frameworks commonly

applied in larger financial institutions (Wang, Xu, Ma, Yang, & Dong, 2025). Consequently, the literature emphasizes that vulnerability assessment cannot be uniformly applied across organizations but must be tailored to institutional capacity, governance maturity, and operational context (Wang et al., 2025). In the context of microfinance institutions, effective vulnerability assessment requires integration with managerial decision-making processes, internal control practices, and organizational learning mechanisms that support sustainable risk management (Aghaunor, Eshua, Obah, & Aromokeye, 2025; Rusu & Mantulescu, 2025).

Simplified yet context-aware vulnerability assessment approaches enable microfinance institutions to manage accounting data security risks in a realistic and cost-efficient manner, while remaining aligned with resource limitations and regulatory expectations (Aghaunor et al., 2025; Nguyen et al., 2024; Rusu & Mantulescu, 2025). Such approaches support the protection of accounting data integrity, enhance reporting reliability, and contribute to the long-term resilience of microfinance institutions. This theoretical framework conceptualizes accounting data vulnerability as a socio-technical phenomenon emerging from the interaction between accounting system digitalization and technical, organizational, and managerial constraints. Vulnerability assessment is positioned not as a one-time technical activity, but as an iterative socio-technical process through which microfinance institutions identify, evaluate, and respond to accounting data vulnerabilities under resource constraints. The learning component embedded in the assessment process enables continuous adaptation, ultimately strengthening accounting data protection and organizational resilience. The conceptual relationships among accounting system digitalization, sources of vulnerability, vulnerability assessment, and organizational resilience are illustrated in Figure 1.

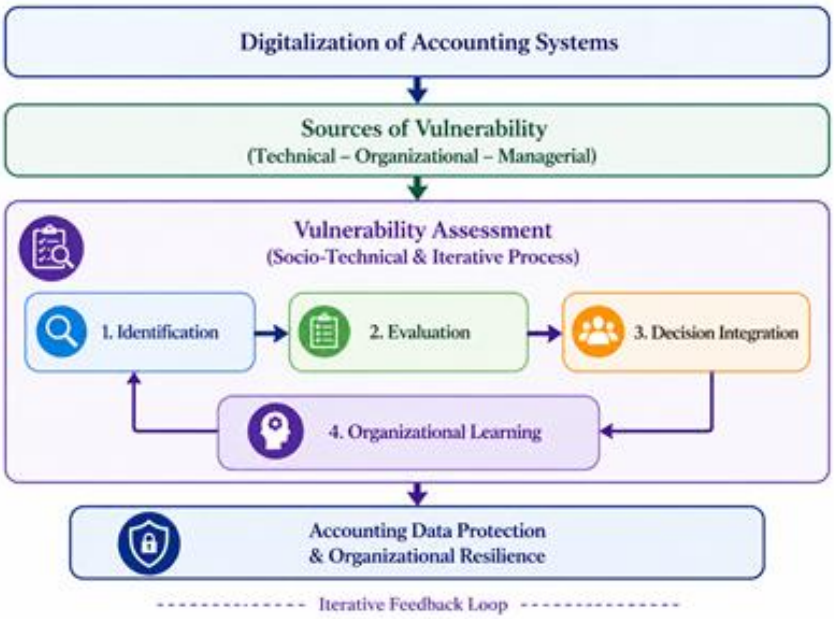

Figure 1. Conceptual framework of accounting data vulnerability assessment in microfinance institutions

3. Methodology

This study employs a multi-case qualitative research design to investigate vulnerabilities in accounting data security and to examine how microfinance institutions utilize vulnerability assessments as a practical approach for evaluating accounting data security. A qualitative approach is employed to capture in-depth processes, practices, and decision-making dynamics that shape vulnerability management under the resource constraints characteristic of microfinance institutions. The research follows an inductive comparative logic, whereby empirical findings across cases are systematically analyzed to identify recurring patterns of vulnerability and vulnerability assessment practices within differing operational contexts (Emkani et al., 2024). The analytical focus is placed on how vulnerabilities are identified and evaluated and how assessment outcomes are translated into managerial actions, rather than on testing causal relationships among variables.

The study involves six microfinance institutions operating in Surakarta, Indonesia, comprising Rural Banks, Islamic Rural Banks, and Savings and Loan Cooperatives. All selected institutions have adopted digital accounting systems and possess experience in managing risks related to accounting data. Case selection was conducted purposively through an initial screening process based on three inclusion criteria: small to medium institutional scale, use of digital accounting systems, and active involvement in accounting data management. The selected cases represent variation in institutional type, organizational scale, and levels of digital accounting adoption, providing a comparative basis for examining vulnerability assessment practices across differing resource conditions. Table 1 provides an overview of the participating microfinance institutions and the profiles of key informants involved in this study.

Table 1. Characteristics of participating institutions and informants

Case	Institution Type	Organizational Scale	Digital Accounting System	Informant Roles	Number of Informants
Case 1	Rural Bank (BPR)	Small-Medium	Core Banking System	Director, Accounting Supervisor, Operations Staff, IT/System Staff	4
Case 2	Rural Bank (BPR)	Small-Medium	Core Banking System	Director, Accounting Supervisor	2
Case 3	Islamic Rural Bank (BPRS)	Small-Medium	Core Banking System	Director, Operations Manager, Head of Accounting, IT Staff	4
Case 4	Islamic Rural Bank (BPRS)	Small-Medium	Core Banking System	Director, Operations Manager, Accounting Staff	3
Case 5	Savings and Loan Cooperative	Small-Medium	Computerized Accounting System	Chairperson, Treasurer, Administrative Officer, Accounting Staff	4
Case 6	Savings and Loan Cooperative	Small-Medium	Computerized Accounting System	Chairperson, Treasurer, Accounting Staff, Administrative Officer	4

Based on the case selection criteria, a total of 21 key informants were recruited from six participating institutions. The informants represented various organizational functions directly involved in the operation, management, and oversight of digital accounting systems. Detailed information regarding the informants' positions, functional areas, and years of professional experience can be seen in Table 2.

Table 2. Informant profile

Informant Code	Institution Type	Position	Functional Area	Experience (Years)
I1	Rural Bank (BPR)	Director	Management	18
I2	Rural Bank (BPR)	Accounting Supervisor	Accounting	12
I3	Rural Bank (BPR)	Operations Staff	Operations	8
I4	Rural Bank (BPR)	IT/System Staff	Information Systems	6
I5	Rural Bank (BPR)	Director	Management	15
I6	Rural Bank (BPR)	Accounting Supervisor	Accounting	10
I7	Islamic Rural Bank (BPRS)	Director	Management	16
I8	Islamic Rural Bank (BPRS)	Operations Manager	Operations	12

I9	Islamic Rural Bank (BPRS)	Head of Accounting	Accounting	11
I10	Islamic Rural Bank (BPRS)	IT Staff	Information Systems	7
I11	Islamic Rural Bank (BPRS)	Director	Management	14
I12	Islamic Rural Bank (BPRS)	Operations Manager	Operations	10
I13	Islamic Rural Bank (BPRS)	Accounting Staff	Accounting	6
I14	Savings and Loan Cooperative	Chairperson	Management	13
I15	Savings and Loan Cooperative	Treasurer	Finance	10
I16	Savings and Loan Cooperative	Administrative Officer	Administration	7
I17	Savings and Loan Cooperative	Accounting Staff	Accounting	5
I18	Savings and Loan Cooperative	Chairperson	Management	12
I19	Savings and Loan Cooperative	Treasurer	Finance	9
I20	Savings and Loan Cooperative	Accounting Staff	Accounting	6
I21	Savings and Loan Cooperative	Administrative Officer	Administration	5

A total of 21 key informants participated in the study, representing managerial, accounting, operational, administrative, and information systems functions across six microfinance institutions. Their professional experience ranged from 5 to 18 years, providing diverse perspectives on digital accounting system implementation and vulnerability assessment practices.

Data collection was conducted through **s**emi-structured in-depth interviews, Focus Group Discussions (FGDs), and document analysis to obtain a comprehensive understanding of accounting data security practices. Interviews involved two to four key informants per case representing managerial, accounting, operational, and system-related roles. FGDs were conducted across cases to capture collective dynamics and to validate emerging patterns. Participants were drawn partly from interview informants and partly from additional organizational members to reduce informant bias and enhance cross-functional perspectives. Document analysis covered accounting procedures, data security policies, technology and infrastructure documentation, audit reports, incident records, and human resource and managerial planning documents to strengthen data triangulation.

Data were analyzed using a layered thematic analysis approach. First, within-case analysis was conducted to develop an in-depth contextual understanding of how vulnerabilities were identified, assessed, and managed within each institution. Coding began with open coding to identify initial categories related to the digital accounting context, vulnerability types, and resource constraints. These categories were then integrated through axial coding, linking vulnerabilities to vulnerability assessment practices and managerial responses. Conditional coding was subsequently applied to interpret how resource constraints shaped the effectiveness of vulnerability assessment in evaluating accounting data security.

To improve analytical transparency, the coding process was documented through a structured coding framework. During open coding, interview transcripts, FGD records, and institutional documents were examined line-by-line to identify meaningful concepts related to accounting data security. Examples of

initial codes included shared user accounts, default passwords, irregular system updates, limited IT budgets, absence of formal security procedures, incident-driven responses, and lack of post-incident documentation. During axial coding, conceptually related codes were grouped into broader categories such as technical security weaknesses, resource limitations, governance deficiencies, reactive risk assessment practices, and organizational learning gaps. Through conditional coding and cross-case comparison, these categories were subsequently synthesized into higher-order themes that explained how resource constraints shaped vulnerability assessment practices across institutions. Table 3 presents an illustration of how representative empirical evidence was transformed into open codes, axial categories, and aggregated themes.

Table 3. Illustration of coding development process

Representative Evidence	Open Codes	Axial Categories	Aggregated Themes
Default passwords and irregular system updates	Default passwords; irregular patching	Technical security weaknesses	Capacity Constraints
Shared user accounts among staff	Shared access; weak access control	Inadequate internal controls	Capacity Constraints
Security actions taken only after incidents occur	Incident-driven response; reactive actions	Informal risk assessment	Reactive Risk Evaluation
No structured criteria for evaluating vulnerabilities	Subjective risk judgment	Reactive evaluation practices	Reactive Risk Evaluation
Security investments decided only after problems emerge	Short-term decisions; cost considerations	Governance limitations	Weak Governance Integration
Assessment results rarely translated into SOPs	Lack of policy formalization	Governance integration gap	Weak Governance Integration
No post-incident review documentation	Missing documentation	Learning deficiencies	Fragmented Organizational Learning
SOPs and manuals rarely updated	Weak knowledge transfer	Organizational learning gaps	Fragmented Organizational Learning

As shown in Table 3, the coding process followed a systematic progression from empirical observations to conceptual abstraction. Initial open codes derived from interviews, FGDs, and documentary evidence were consolidated into axial categories that captured recurring patterns across cases. These categories were then integrated through conditional coding to generate four overarching themes: Capacity Constraints, Reactive Risk Evaluation, Weak Governance Integration, and Fragmented Organizational Learning. These themes subsequently formed the analytical foundation for the cross-case analysis and the development of the proposed vulnerability assessment model.

Next, cross-case analysis was performed to compare thematic patterns across institutions with differing levels of resource constraints. The findings reveal that variations in resource capacity influence the depth of vulnerability assessment, the degree of decision formalization, and the intensity of organizational learning. The coding results demonstrate that technical, organizational, and managerial vulnerabilities interact dynamically, positioning vulnerability assessment as a socio-technical process mediated by resource limitations and managerial practices.

Analytical rigor was enhanced through data triangulation, the involvement of two independent coders, convergence discussions to align interpretations, and member checking to ensure that the derived

themes accurately reflected empirical realities. Overall, the methodological approach provides a robust and coherent foundation for exploring accounting data security vulnerabilities and understanding the practical use of vulnerability assessment in microfinance institutions. The integration of a multi-case design, multiple data sources, and layered thematic analysis ensures strong analytical validity, empirical depth, and practical relevance for strengthening accounting data security and organizational resilience.

To support cross-case comparison, institutional capacity was assessed using four dimensions: IT and security budget, human resource capacity, digital infrastructure, and security policy and training. Scores were assigned based on triangulated evidence obtained from interviews, focus group discussions, and document analysis. Each institution was evaluated against predefined criteria for each dimension, and the final scores were determined through researcher consensus to ensure consistency across cases.

4. Results and Discussions

4.1 Fragmented Digitalization as a Source of Vulnerability

The findings indicate that digitalization in microfinance institutions has been widely adopted but remains uneven in terms of system integration and maturity. Digitalization is generally understood as the use of accounting software or core banking systems to support transaction recording, financial reporting, and regulatory compliance. However, the implementation does not yet reflect full system integration. As stated by a Rural Bank Director during the interview, "*At the end of each month, we still export transaction data from the core banking system into spreadsheets before preparing the financial reports. Because several staff members handle the files, mistakes sometimes happen, and there is no automatic validation process to detect them"* (I10, IT Staff, Islamic Rural Bank). Similarly, the Treasurer of a savings and loan cooperative explained, *"For several regulatory and management reports, we still had to combine data from different modules manually. The process required additional checking because inconsistencies sometimes appeared between the system records and the reports generated for management."* (I15, Treasurer, Savings and Loan Cooperative).

These accounts illustrate that accounting data processing continues to rely on manual data transfers despite the adoption of digital systems. Similar experiences were reported across different institutional types, suggesting that fragmented system integration remains a recurring challenge in microfinance institutions. The absence of automated validation mechanisms increases the risk of data inconsistencies and reduces the reliability of financial reporting processes.

This condition indicates that digitalization in microfinance institutions remains partial and fragmented, creating structural vulnerabilities in accounting data processing and increasing the risk of data inconsistency and unauthorized manipulation. Despite the adoption of digital systems, several processes continue to rely on manual intervention, particularly during reconciliation and reporting stages. This hybrid system not only increases operational workload but also amplifies the risk of errors and data security breaches due to cross-system data transfers.

The findings reveal a strong dependence on external vendors across different types of microfinance institutions, indicating a critical shift in control over accounting systems and data security. Rural Banks and Islamic Rural Banks generally relied on core banking systems provided by external vendors. *"Whenever a technical problem occurred, we could not immediately investigate the issue because only the vendor had administrative access to the system. We had to wait for their response before any corrective action could be taken, which sometimes delayed operational activities."* (I9, Head of Accounting, Islamic Rural Bank). This observation was reinforced by an Accounting Supervisor of a Rural Bank who noted, "*Most system configurations, security settings, and software updates were handled entirely by the vendor. Internally, we did not have sufficient technical knowledge to verify whether the security controls were functioning properly*" (I2, Accounting Supervisor, Rural Bank).

These accounts suggest that dependence on external vendors extends beyond technical support and influences the institution's ability to independently manage and evaluate accounting data security. Limited access to system administration and security configurations reduces organizational control over critical processes and may hinder timely responses to emerging vulnerabilities.

Similarly, savings and loan cooperatives also depended on vendor-provided accounting systems. The Chairperson of a savings and loan cooperative explained, *"Most security settings were configured by the vendor, and we did not fully understand how they worked. If there was a problem with the system, we usually waited for the vendor to diagnose and resolve it because we lacked the technical capability to do so ourselves"* (I14, Chairperson, Savings and Loan Cooperative). This reliance indicates that system configuration, software updates, and accounting data security are largely delegated to external providers, reducing institutional control over critical technical and security functions. Similar patterns were observed across Rural Banks, Islamic Rural Banks, and Savings and Loan Cooperatives, suggesting that vendor dependency represents a recurring source of vulnerability in resource-constrained microfinance institutions. Across all six institutions, vulnerability was not primarily driven by the absence of digital systems, but by limited organizational control over those systems and the institutional capacity required to manage them effectively.

The findings also indicate limited internal organizational capacity in managing accounting systems, particularly in terms of documentation and knowledge transfer. Although most institutions possessed system manuals or guidelines, these documents were not regularly updated and were rarely used in daily operations. An Operations Manager of an Islamic Rural Bank stated, "*Most staff learned how to operate the system from senior colleagues rather than from the official manuals. When system updates were introduced, employees often relied on informal explanations because the documentation had not been updated accordingly*" (I8, Operations Manager, Islamic Rural Bank). Similarly, an Administrative Officer of a savings and loan cooperative explained, "*The manuals were provided by the vendor, but they were rarely consulted in daily work. New employees usually learned through direct guidance from existing staff, and some procedures were not formally documented*" (I16, Administrative Officer, Savings and Loan Cooperative). These accounts suggest that organizational knowledge related to accounting systems remains largely informal and person-dependent. As a result, critical knowledge is not consistently retained within the organization, increasing operational risks when staff turnover occurs or when significant system changes are introduced.

This condition is further reflected in the low level of staff understanding, particularly when system changes were introduced by vendors. An administrative officer noted that internal comprehension of SOPs remained limited, especially during system updates. This indicates that knowledge related to accounting systems is not effectively internalized, increasing dependence on vendors and weakening organizational resilience in managing accounting data security. Overall, the findings suggest that digitalization in microfinance institutions is characterized not only by technological adoption but also by structural dependence on external vendors and limited internal capability. While digital systems improve operational efficiency, they simultaneously shift control over accounting processes and data security to external parties and expose organizations to new forms of vulnerability. This highlights the importance of integrating technical systems with organizational capacity in developing effective vulnerability assessment practices.

4.2 Sources of Accounting Data Vulnerability in Microfinance Institutions

The findings reveal that accounting data security vulnerability in microfinance institutions is primarily shaped by variations in institutional resource capacity, which determine the extent of technical, organizational, and managerial vulnerabilities. Institutional capacity was assessed using four dimensions: IT and security budget, human resource capacity, digital infrastructure, and security policy and training. The assessment employed a four-point ordinal scale ranging from 0 (High Capacity) to 3 (Very Low Capacity). Scores were assigned based on triangulated evidence obtained from interviews, focus group discussions, and document analysis. Each dimension was evaluated against predefined qualitative criteria reflecting the availability of resources, level of formalization, and degree of implementation. To enhance consistency, scoring decisions were discussed and agreed upon by the research team through coder consensus. Table 4 presents the assessment criteria used for institutional capacity scoring by (Bennouk et al., 2024; El-Hajj & Mirza, 2024; Wang et al., 2025).

Table 4. Institutional capacity assessment criteria

Dimension	Score 0 (High)	Score 1 (Moderate)	Score 2 (Low)	Score 3 (Very Low)
IT & Security Budget	Dedicated annual security budget	Budget available but limited	Minimal budget allocation	No dedicated budget
HR Capacity	Dedicated IT/security personnel with regular training	Basic IT personnel available	Limited IT expertise	No dedicated IT expertise
Digital Infrastructure	Integrated systems with security controls	Moderate infrastructure	Basic infrastructure	Highly limited infrastructure
Security Policy & Training	Formal policies and periodic training	Policies exist but are partially implemented	Informal procedures	No policy and no training

The scores presented in Table 5 were assigned based on the institutional capacity criteria described in Table 4. Institutions receiving higher scores generally exhibited limited security investment, weaker governance mechanisms, lower levels of staff competency, and less mature digital infrastructure. Conversely, lower scores reflected stronger organizational capacity and more formalized security management practices. For example, institutions assigned a score of 0 for digital infrastructure operated integrated core banking systems with established security controls, whereas institutions assigned a score of 3 relied on basic accounting systems with limited security features and minimal system integration.

Table 5. Institutional capacity scores related to accounting data security in microfinance institutions

Type of Institution	IT & Security Budget	HR Capacity	Digital Infrastructure	Security Policy & Training
Rural Bank	Score 1 (Moderate)	Score 1 (Moderate)	Score 1 (Moderate)	Score 1 (Moderate)
Rural Bank	Score 1 (Moderate)	Score 2 (Low)	Score 2 (Low)	Score 2 (Low)
Islamic Rural Bank	Score 0 (High)	Score 1 (Moderate)	Score 0 (High)	Score 1 (Moderate)
Islamic Rural Bank	Score 2 (Low)	Score 2 (Low)	Score 2 (Low)	Score 3 (Very Low)
Savings and loan cooperative	Score 3 (Very Low)	Score 2 (Low)	Score 2 (Low)	Score 3 (Very Low)
Savings and loan cooperative	Score 3 (Very Low)	Score 3 (Very Low)	Score 3 (Very Low)	Score 3 (Very Low)

The capacity assessment results provide an empirical basis for understanding why vulnerability patterns differ across institutions and help explain variations in technical, organizational, and managerial vulnerabilities. Table 5 shows a clear pattern in which institutions with lower resource capacity tend to be more vulnerable across all dimensions, particularly in IT infrastructure, human resources, and security governance. Limited security infrastructure and weak IT management capacity lead to predominantly reactive security practices, where actions are triggered by incidents rather than guided by preventive and systematic mechanisms. Security policies are often undocumented, risk management responsibilities are unclear, and decisions are driven by short-term priorities. Consequently, security efforts are reactive and unstructured, lacking sustainable preventive strategies.

This pattern is reinforced by interview evidence. A Director of a Rural Bank explained, *"When a system disruption or data access problem occurred, management usually discussed the issue only after operations had been affected. We would hold a meeting to identify the immediate cause and decide on corrective actions, but there was rarely a formal review process to document lessons learned or prevent similar incidents from happening again"* (I1, Director, Rural Bank). This reflects a lack of structured

organizational learning, where post-incident evaluations are not institutionalized and continuous improvement mechanisms are largely absent.

The findings demonstrate that accounting data security vulnerability in microfinance institutions can be conceptualized into three interrelated dimensions: technical, organizational, and managerial vulnerabilities. These dimensions consistently emerged across in-depth interviews, focus group discussions, and institutional document analysis.

1. Technical vulnerability emerged as the most critical dimension, particularly in institutions with limited digital infrastructure and IT budgets. Interview and document findings indicated that technical vulnerabilities included the use of default passwords, irregular system updates and patching, limited antivirus functionality, and inconsistent or untested data backup mechanisms. An Accounting Supervisor of a Rural Bank explained, *"Several employees still used the default passwords provided when the system was first installed because password changes were not routinely enforced. System updates were usually performed only when problems occurred, and we rarely tested whether backup files could actually be restored if the system failed"* (I2, Accounting Supervisor, Rural Bank). In small-scale cooperatives and rural banks, standalone accounting systems or systems with only basic security controls increased the risk of system disruption and accounting data loss. Furthermore, user access settings that were not role-based resulted in multiple staff members using a single account, thereby increasing the risk of access misuse and obscuring audit trails. The Head of Accounting of an Islamic Rural Bank stated, *"During busy operational periods, several staff members often shared the same user account because access permissions were not assigned according to specific roles. When discrepancies appeared in transaction records, it was difficult to determine who had performed a particular activity because the audit trail did not clearly identify individual users"* (I9, Head of Accounting, Islamic Rural Bank). These technical vulnerabilities were further reinforced by strong dependence on external vendors, particularly for security configuration and software maintenance, which limited institutions' ability to conduct independent security evaluations. Similar technical weaknesses were reported across Rural Banks, Islamic Rural Banks, and Savings and Loan Cooperatives, although their severity varied according to institutional resource capacity.
2. Organizational vulnerability reflects weak governance structures in managing accounting data security. Document analysis showed that, in several institutions, security procedures remained implicit and were not formally embedded in accounting standard operating procedures. As noted by an Operations Manager of an Islamic Rural Bank, "*We had procedures for daily accounting operations, but there was no specific SOP that clearly defined responsibilities and controls related to accounting data security. Most security-related actions depended on individual experience and managerial instructions rather than documented procedures*" (I8, Operations Manager, Islamic Rural Bank). As a result, data security practices were largely reactive, emerging only in response to system disruptions or audit findings. Focus group discussions further indicated that cross-functional coordination in managing data security risks was limited. An Accounting Staff member of a Savings and Loan Cooperative explained, "*Different departments handled security issues separately, and there were no regular meetings to discuss potential risks or review security incidents. When problems occurred, they were usually resolved within individual units without formal documentation or follow-up evaluation*" (I17, Accounting Staff, Savings and Loan Cooperative). In addition, the absence of systematic evaluation and structured organizational learning undermined the documentation and effective utilization of vulnerability assessment outcomes for continuous improvement. These findings indicate that vulnerability management was not institutionalized, thereby limiting the effectiveness of preventive and sustainable security practices. These governance-related challenges were observed across all institutional types, suggesting that organizational vulnerability is not limited to technological constraints but also reflects weaknesses in formal governance mechanisms.
3. Managerial vulnerability was related to leadership priorities and decision-making patterns concerning accounting data security. Interviews with leaders and managers revealed that short-term considerations, including cost efficiency and daily operational pressures, often influenced decisions regarding security investments. A Director of an Islamic Rural Bank stated, "When annual budgets were discussed, lending expansion and operational activities usually received higher priority than

cybersecurity investments because management expected more immediate returns from those expenditures" (I11, Director, Islamic Rural Bank). Accounting data security was often viewed as a technical issue rather than a strategic risk that affects organizational sustainability. The Chairperson of a Savings and Loan Cooperative explained, *"Management discussions mainly focused on operational performance and member services. Data security was usually discussed only when a system problem affected daily operations, so it rarely became part of long-term strategic planning"* (I14, Chairperson, Savings and Loan Cooperative). In many cases, vulnerability assessment was not utilized as a systematic managerial instrument but rather as a response to incidents or external recommendations. An Administrative Officer of a Savings and Loan Cooperative stated, *"We normally reviewed security controls only after audit findings, system disruptions, or vendor recommendations. There was no formal schedule for assessing vulnerabilities or evaluating whether existing controls remained effective."* (I16, Administrative Officer, Savings and Loan Cooperative). Across the six institutions, managerial responses to accounting data security were predominantly reactive, indicating that vulnerability assessment has not yet been fully integrated into strategic decision-making processes.

4.3 Vulnerability Assessment in Microfinance Institutions

The proposed process-based vulnerability assessment model begins with capacity-based identification, followed by vulnerability evaluation, managerial decision integration, and organizational learning. Each stage reflects the empirical conditions observed in microfinance institutions, where limited resources, reactive practices, weak governance integration, and fragmented learning constrain the effectiveness of vulnerability assessment. The model directly addresses the empirical weaknesses identified in Rural Banks, Islamic Rural Banks, and savings and loan cooperative, providing a structured and context-sensitive framework that strengthens the institutionalization of vulnerability assessment in accounting data security. The empirical findings were synthesized into four aggregated themes representing the sequential stages of the proposed vulnerability assessment process, as presented in Table 6.

Table 6. Aggregated themes and process stages of the vulnerability assessment in microfinance institutions

Aggregated Theme	Representative Empirical Indicators	Process Stage
Capacity Constraints	Limited IT security budget, basic system protection, shared user access, low IT literacy, and absence of formal SOPs	Capacity-Based Identification
Reactive Risk Evaluation	Incident-driven assessment, informal risk judgment, and lack of structured evaluation criteria	Vulnerability Evaluation
Weak Governance Integration	Post-incident managerial meetings, ad hoc decisions, and limited policy formalization	Managerial Decision Integration
Fragmented Organizational Learning	No post-incident documentation, SOP not updated, knowledge remains individual	Organizational Learning

Based on the empirical findings and the theoretical framework presented in Figure 1, a process-based vulnerability assessment model was developed and is presented in Figure 2.

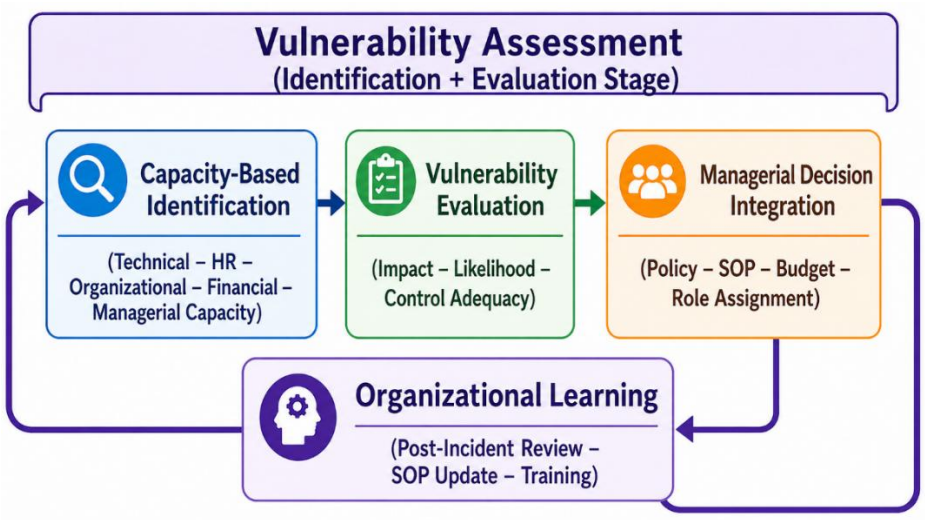

Figure 2. Proposed process-based vulnerability assessment model for accounting data security in microfinance institutions

The proposed model not only conceptualizes the vulnerability assessment process but also provides practical guidance for its implementation in resource-constrained microfinance institutions. To support decision-making, vulnerabilities identified during the assessment process should be systematically prioritized according to their potential consequences and probability of occurrence. Prioritization is particularly important in institutions with limited financial, technological, and human resources, as it enables managers to allocate corrective actions more effectively. Accordingly, Table 7 presents a practical vulnerability risk matrix that can be used to classify identified vulnerabilities and determine appropriate response priorities.

Table 7. Practical vulnerability risk matrix

Likelihood	Impact	Risk Level	Recommended Action
High	High	Critical	Immediate mitigation
High	Medium	High	Correct within 30 days
Medium	Medium	Moderate	Monitor and improve
Low	Low	Low	Routine monitoring

To facilitate practical implementation, identified vulnerabilities may be prioritized using a simple risk matrix that weights likelihood of occurrence against the potential impact on the confidentiality, integrity, and availability of accounting data. This approach enables resource-constrained institutions to focus their limited resources on the most critical vulnerabilities. To enhance usability, each stage of the proposed model can be translated into specific managerial activities and outputs, as shown in Table 8. This operational guidance enables institutions to systematically implement vulnerability assessment despite resource constraints.

Table 8. Operational guidance for implementing the proposed model

Stage	Key Activities	Expected Output
Capacity-Based Identification	Assess budget, HR, infrastructure, policies	Capacity profile
Vulnerability Evaluation	Assess likelihood, impact, control adequacy	Risk priority list
Managerial Decision Integration	Determine corrective actions and allocate resources	Action plan
Organizational Learning	Document incidents and update SOPs	Organizational learning record

While Table 8 specifies the key activities and expected outputs for each stage of the proposed model, managers also require a practical mechanism to assess whether these activities have been adequately implemented. Therefore, Table 9 presents an accounting data security self-assessment checklist that operationalizes the proposed model into a set of guiding questions covering key technical, organizational, and managerial controls.

Table 9. Accounting data security self-assessment checklist

Assessment Area	Guiding Question
Password Management	Are default passwords still used?
User Access Control	Are user accounts assigned individually?
System Updates	Are security patches applied regularly?
Data Backup	Are backup files tested periodically?
Security Policies	Is a documented security SOP available?
Staff Training	Have employees received security training within the last year?
Incident Review	Are security incidents formally documented and reviewed?

The checklist may serve as a preliminary self-assessment tool for managers of microfinance institutions. Institutions that answer "No" to multiple questions should prioritize corrective actions and conduct a more comprehensive vulnerability assessment. The four-stage model directly addresses the empirical weaknesses identified in this study. Capacity-Based Identification responds to resource limitations observed across institutions, Vulnerability Evaluation addresses the prevalence of reactive and informal risk assessment practices, Managerial Decision Integration strengthens the linkage between vulnerability assessment and strategic decision-making, and Organizational Learning mitigates the absence of systematic documentation and post-incident evaluation. Consequently, the model translates empirical findings into a practical framework that can support continuous improvement in accounting data security management.

4.4 Discussion

This study provided empirical insights into how vulnerability assessment was practiced within microfinance institutions operating under significant resource constraints. Rather than functioning as a standardized or fully institutionalized security mechanism, vulnerability assessment in these institutions emerged as a reactive, capacity-driven, and weakly integrated socio-technical process. The findings extended prior cybersecurity and accounting information systems literature by demonstrating that vulnerabilities in microfinance institutions were not merely technical deficiencies but were deeply embedded in organizational structures, managerial decision-making, and learning practices.

The findings highlighted that capacity constraints constituted the primary entry point of vulnerability assessment in microfinance institutions. Limitations in IT security budgets, digital infrastructure, human resource competencies, and formal governance mechanisms shaped how vulnerabilities were initially recognized. Unlike large financial institutions that employ formal vulnerability scanning tools and dedicated security teams, the institutions examined in this study identified vulnerabilities implicitly through operational disruptions and system limitations. This finding reinforced prior studies suggesting that vulnerability in small financial institutions is structurally conditioned by resource availability rather than isolated technological flaws (El-Hajj & Mirza, 2024; Lwesya & Mwakalobo, 2023). Consequently, vulnerability assessment in microfinance contexts tended to be experiential and situational rather than analytical and systematic.

The results demonstrated that vulnerability evaluation was predominantly conducted through reactive and informal risk assessment practices. Risk judgments were largely incident-driven and relied on managerial intuition instead of predefined evaluation criteria or risk matrices. This pattern was consistent with earlier research indicating that microfinance institutions often respond to security risks only after system failures or audit findings occur (Aghaunor et al., 2025; Rusu & Mantulescu, 2025). As a result, vulnerability evaluation did not effectively support proactive prioritization of mitigation measures, limiting its strategic value for accounting data protection.

The findings revealed that managerial decision integration represented a critical bottleneck in the vulnerability assessment process. Although security incidents frequently triggered managerial discussions, the outcomes of these discussions were rarely formalized into updated policies, standard operating procedures, or dedicated security budgets. This finding aligned with organizational vulnerability literature, which emphasizes that weak governance integration reduces the sustainability of risk mitigation efforts (Bennouk et al., 2024). The tendency to frame accounting data security as a technical or operational issue, rather than a strategic organizational risk, further constrained managerial commitment to long-term security investments (Offiong et al., 2024).

The study found that organizational learning remained fragmented, significantly limiting the effectiveness of vulnerability assessment over time. The lack of structured post-incident reviews, formal documentation, and systematic SOP updates meant that lessons learned from security incidents were not converted into institutional knowledge. This finding aligns with organizational resilience research, which emphasizes that learning loops are essential for converting ad hoc responses into durable organizational capabilities. Without institutionalized learning mechanisms, vulnerability management efforts tended to be temporary, allowing similar security weaknesses to recur.

By integrating these empirical findings, this study developed a process-based vulnerability assessment model consisting of four iterative stages: capacity-based identification, vulnerability evaluation, managerial decision integration, and organizational learning. The model contributed theoretically by reframing vulnerability assessment in microfinance institutions as a dynamic governance process rather than a purely technical exercise. It also responded directly to calls in the literature for context-sensitive security frameworks tailored to resource-constrained financial institutions (Isa et al., 2024; Waweru et al., 2024).

From a practical perspective, the discussion underscored that the proposed model addressed key empirical weaknesses observed in Rural Banks, Islamic Rural Banks, and savings and loan cooperative. Systematic capacity mapping enabled institutions to prioritize mitigation actions more cost-effectively, while the integration of assessment outcomes into formal governance structures supported a shift from reactive to preventive security practices. Furthermore, embedding organizational learning as a feedback mechanism strengthened institutional memory and enhanced adaptive capacity, even in environments characterized by limited resources. These implications were consistent with prior findings linking capacity-oriented interventions to improved accounting data reliability and organizational resilience (Lwesya & Mwakalobo, 2023; Pattnaik et al., 2024; Siakas, Naaranoja, Vlachakis, & Siakas, 2014). Overall, vulnerability assessment in microfinance institutions must be understood as a socio-technical and iterative process shaped by structural constraints and managerial practices. The proposed model offered a realistic and empirically grounded pathway for strengthening accounting data security and organizational resilience, contributing both theoretically and practically to the growing body of literature on cybersecurity and accounting systems in microfinance contexts.

5. Conclusions

5.1 Conclusion

This study set out to examine how accounting data vulnerabilities emerge in microfinance institutions and how vulnerability assessment is practiced under resource constraints. The findings demonstrate that vulnerabilities are not solely technical issues but arise from the interaction of limited digital infrastructure, human resource constraints, weak governance structures, and short-term managerial decision-making. Vulnerability assessment practices are largely reactive, informal, and weakly embedded in organizational processes. To address these conditions, this study develops a process-based vulnerability assessment model consisting of four interrelated stages: capacity-based identification, vulnerability evaluation, managerial decision integration, and organizational learning. The model highlights that vulnerability assessment should be understood as an iterative socio-technical process, where organizational learning plays a critical role in strengthening continuous improvement. These findings contribute to a broader understanding of accounting data security by shifting the perspective from purely technical approaches to governance-driven and context-sensitive frameworks, particularly relevant for microfinance institutions.

5.2 Research Limitations

This study has several limitations. First, it is based on a limited number of cases within a specific regional context, which may restrict the generalizability of the findings. Second, the analysis primarily reflects internal organizational perspectives and does not incorporate insights from regulators, external auditors, or technology vendors. Third, the qualitative approach, while providing in-depth insights, does not allow for statistical generalization or measurement of the model's effectiveness. Based on these limitations, future improvements may include expanding institutional diversity, incorporating external stakeholder perspectives, and combining qualitative insights with quantitative validation to strengthen the robustness of the findings.

5.3 Suggestions and Directions for Future Research

Future research is encouraged to test and validate the proposed model across broader geographical contexts and different types of financial institutions to enhance its generalizability. Researchers may also adopt mixed-method approaches to quantitatively assess the impact of vulnerability assessment practices on reducing security incidents and improving financial reporting reliability. In addition, further studies can explore the role of regulatory frameworks, digital governance, and technological innovation, such as automated security tools or AI-based risk detection, in strengthening vulnerability assessment practices. Examining the integration of organizational learning mechanisms into formal governance systems also offers a promising avenue for advancing both theory and practice in accounting data security and organizational resilience

Acknowledgement

The authors would like to express their sincere appreciation to all participating microfinance institutions and interview informants for their time, openness, and cooperation during the data collection process. The authors also acknowledge the valuable support and constructive feedback provided by colleagues and reviewers, which contributed to the improvement of this article.

Author Contributions

AW contributed to the conceptualization, study design, data collection, data analysis, and manuscript drafting. MK was responsible for methodology development, validation, supervision, and manuscript revision. KHT contributed to data collection, data analysis, literature review, and manuscript drafting. All authors participated in the final review and approved the final version of the manuscript.

References

Adejumo, A., & Ogburie, C. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews, 25*(3), 1527-1541. doi:https://doi.org/10.30574/wjarr.2025.25.3.0908

Aghaunor, C. T., Eshua, P., Obah, T., & Aromokeye, O. (2025). Data security strategies to avoid data breaches in modern information systems. *World Journal of Advanced Research and Reviews, 25*(01), 827-849. doi:https://doi.org/10.30574/wjarr.2023.20.3.2515

Andromeda, A., Wahyuni, S., Tubastuvi, N., & Santoso, S. B. (2026). Financial factors determinant to MSME performance. *Jurnal Akuntansi, Keuangan, dan Manajemen, 7*(2), 139-155. doi:https://doi.org/10.35912/jakman.v7i2.5352

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A. Z., & Mahouachi, D. (2024). A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *Journal of Cybersecurity and Privacy, 4*(4), 853-908. doi:https://doi.org/10.3390/jcp4040040

Bukari, C., Koomson, I., & Annim, S. K. (2024). Financial inclusion, vulnerability coping strategies and multidimensional poverty: Does conceptualisation of financial inclusion matter? *Review of Development Economics, 28*(2), 462-498. doi:https://doi.org/10.1111/rode.13062

Calvo-Manzano, J. A., San Feliu, T., Herranz, Á., Mariño, J., Fredlund, L. Å., & Moreno, A. M. (2025). CyberESP: An integrated cybersecurity framework for SMEs. *Journal of Software: Evolution and Process, 37*(9), e70050. doi:https://doi.org/10.1002/smr.70050

Chotia, V., Khoualdi, K., Broccardo, L., & Yaqub, M. Z. (2025). The role of cyber security and digital transformation in gaining competitive advantage through Strategic Management Accounting. *Technology in Society, 81*, 102851. doi:https://doi.org/10.1016/j.techsoc.2025.102851

Damayanti, R., Hamidah, R. A., & Titisari, K. H. (2026). Integrative model of financial literacy, social entrepreneurship, and pentahelix collaboration on MSME performance. *Jurnal Akuntansi, Keuangan, dan Manajemen, 7*(2), 157-171. doi:https://doi.org/10.35912/jakman.v7i2.5542

El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. *Electronics, 13*(19), 3910. doi:https://doi.org/10.3390/electronic13193910

Emkani, M., Yazdi, M., Zarei, E., Klockner, K., Alimohammadlou, M., & Kamalinia, M. (2024). Advancing understanding of vulnerability assessment in process industries: A systematic review of methods and approaches. *International Journal of Disaster Risk Reduction, 107*, 104479. doi:https://doi.org/10.1016/j.ijdrr.2024.104479

Giessmann, A., & Legner, C. (2013). Designing business models for platform as a service: towards a design theory.

Gou, C., & Deng, X. (2023). A blockchain-based security model for cloud accounting data. *International Journal of Ambient Computing and Intelligence (IJACI), 14*(1), 1-16. doi:https://doi.org/10.4018/IJACI.332860

Gupta, A., Mishra, S., & Behera, D. K. (2024). Tracing the trajectory of financial vulnerability: a systematic review and bibliometric analysis. *Cogent Economics & Finance, 12*(1), 2411566. doi:https://doi.org/10.1080/23322039.2024.2411566

Isa, M., Praswati, A. N., & Zulaekah, S. (2024). Vulnerability analysis: A tool for SMEs' business resilience. *IDRiM Journal, 14*(2), 157-175. doi:https://doi.org/10.5595/001c.125616

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications, 241*, 122697. doi:https://doi.org/10.1016/j.eswa.2023.122697

Jiang, Y., Oo, N., Meng, Q., Lim, H. W., & Sikdar, B. (2025). A survey on vulnerability prioritization: Taxonomy, metrics, and research challenges. *arXiv preprint arXiv:2502.11070*. doi:https://doi.org/10.48550/arXiv.2502.11070

Lwesya, F., & Mwakalobo, A. B. S. (2023). Frontiers in microfinance research for Small and Medium Enterprises (SMEs) and Microfinance Institutions (MFIs): a bibliometric analysis. *Future Business Journal, 9*(1), 17. doi:https://doi.org/10.1186/s43093-023-00195-3

Mirtaheri, S. L., Pugliese, A., & Pascucci, V. (2025). Automated vulnerability score prediction through lightweight generative AI. *Knowledge-Based Systems*, 114406. doi:https://doi.org/10.1016/j.knosys.2025.114406

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management, 18*(1), 41. doi:https://doi.org/10.3390/jrfm18010041

Neri, M., Niccolini, F., & Rosario, P. (2022). Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey. *The Online Journal Of Applied Knowledge Management, 10*(2), 1-22. doi:https://doi.org/10.36965/OJAKM.2022.10(2)1-22

Nguyen, P.-H., Nguyen, L.-A. T., Pham, H.-A. T., Nguyen, T.-H. T., & Vu, T.-G. (2024). Assessing cybersecurity risks and prioritizing top strategies In Vietnam's finance and banking system using strategic decision-making models-based neutrosophic sets and Z number. *Heliyon, 10*(19). doi:https://doi.org/10.1016/j.heliyon.2024.e37893

Nurwanah, A. (2024). Cybersecurity in accounting information systems: Challenges and solutions. *Advances in Applied Accounting Research, 2*(3), 157-168. doi:https://doi.org/10.60079/aaar.v2i3.336

Offiong, U. P., Szopik-Depczyńska, K., Cheba, K., & Ioppolo, G. (2024). FinTech as a digital innovation in microfinance companies-systematic literature review. *European Journal of Innovation Management, 27*(9), 562-581. doi:https://doi.org/10.1108/EJIM-04-2024-0462

Pattnaik, D., Ray, S., & Hassan, M. K. (2024). Microfinance: A bibliometric exploration of the knowledge landscape. *Heliyon, 10*(10). doi:https://doi.org/10.1016/j.heliyon.2024.e31216

Raju, A. B. A. (2023). Vulnerability assessment and management in financial software. *International Journal for Multidisciplinary Research, 5*(5). doi:https://doi.org/10.36948/ijfmr.2023.v05i05.12152

Roup, A., & Effendy, M. (2025). Risk analysis of accounting information system security based on vulnerability data from OPENVAS, OWASP ZAP, And NMAP Tools: A Cybersecurity Perspective. *Jurnal Ilmiah Akuntansi Kesatuan, 13*(3), 433-438. doi:https://doi.org/10.37641/jiakes.v13i3.3590

Rusu, D., & Mantulescu, M. (2025). Development of an application-based framework for information security management in SMEs. *Sustainability, 17*(18), 8314. doi:https://doi.org/10.3390/su17188314

Šafár, L., Pekarčik, M., Morawiec, P., Rutecka, P., & Wieczorek-Kosmala, M. (2025). Mapping cybersecurity in SMEs: the role of ownership and firm characteristics in the silesian region of Poland. *Information, 16*(7), 590. doi:https://doi.org/10.3390/info16070590

Shimizu, N., & Hashimoto, M. (2026). Vulnerability management chaining: An integrated framework for efficient cybersecurity risk prioritization. *IEEE Access*. doi:https://doi.org/10.48550/arXiv.2506.01220

Siakas, K., Naaranoja, M., Vlachakis, S., & Siakas, E. (2014). Family businesses in the new economy: How to survive and develop in times of financial crisis. *Procedia Economics and Finance, 9*, 331-341. doi:https://doi.org/10.1016/S2212-5671(14)00034-3

Torkamani, M. J., Ng, J., Mehrotra, N., Chandramohan, M., Krishnan, P., & Purandare, R. (2025). Streamlining security vulnerability triage with large language models. *arXiv preprint arXiv:2501.18908*. doi:https://doi.org/10.48550/arXiv.2501.18908

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv preprint arXiv:2503.22710*. doi:https://doi.org/10.63125/fh49gz18

Wang, Y., Xu, S., Ma, C., Yang, Q., & Dong, Y. (2025). *Development and trend of service security management under big data technology.* Paper presented at the Proceedings of the 2025 2nd International Conference on Innovation Management and Information System.

Waweru, E., Karume, S. M., & Kibet, A. (2024). A review of human vulnerabilities in cyber security: Challenges and solutions for microfinance institutions. *Journal of Information Security, 16*(1), 114-130. doi:https://doi.org/10.4236/jis.2025.161006

Wijayanti, P., Mohamed, I. S., & Daud, D. (2024). Computerized accounting information systems: An application of task technology fit model for microfinance. *International Journal of Information Management Data Insights, 4*(1), 100224. doi:https://doi.org/10.1016/j.jjimei.2024.100224

Zlati, M. L., Ionescu, R. V., & Antohi, V. M. (2022). Modelling the vulnerability of financial accounting systems during global challenges: A comparative analysis. *Mathematics, 10*(9), 1462. doi:https://doi.org/10.3390/math10091462