Profixa: International Journal of Economic and Business Research
Vol 1 No 2 April 2026, Hal 01-09
ISSN: 3124-3738 (Print) ISSN: 3124-372X(Electronic)
Open Access: https://researchfrontiers.id/profixa/index

Balancing Innovation and Risk: Cybersecurity Concerns in Cloud Adoption Among Accountants

Iis Solihat[1*]
[1] Open University, Indonesia
email: isolihat@ecampus.ut.ac.id[1]

Article Info :
Received:
20-03-2026
Revised:
28-03-2026
Accepted:
03-04-2026

Abstract

The rapid advancement of digital technology has significantly transformed the accounting profession, particularly through the adoption of cloud computing. While cloud accounting offers substantial benefits such as improved efficiency, real-time data access, and cost-effectiveness, it also introduces critical cybersecurity risks that may hinder its adoption. This study aims to examine how accountants balance the benefits of innovation with cybersecurity concerns in adopting cloud-based accounting systems. This research employs a qualitative approach using focus group discussions and in-depth interviews with accounting professionals. The analysis is guided by the cybersecurity risk taxonomy framework, encompassing individual actions, system and technology failures, internal process weaknesses, and external threats. Thematic analysis is applied to identify key patterns and insights related to cloud adoption behavior. The findings reveal that although cloud accounting enhances financial reporting efficiency, accuracy, and timeliness, cybersecurity concerns particularly data breaches, unauthorized access, and system vulnerabilities remain significant barriers to adoption. Additionally, perceived trust and cybersecurity awareness play a crucial mediating role in influencing adoption decisions. Higher levels of trust and security awareness are associated with greater acceptance and effective implementation of cloud accounting systems. This study contributes to the literature by integrating perspectives of cybersecurity risk and trust in understanding cloud accounting adoption. Practically, the findings highlight the importance of strengthening cybersecurity frameworks, enhancing user awareness, and implementing comprehensive risk management strategies to support secure and sustainable adoption of cloud technologies in the accounting profession.

Keywords: *Cloud Accounting, Cybersecurity, Digital Transformation, Financial Reporting Quality, Trust.*

INTRODUCTION

The global accounting landscape is undergoing a profound transformation driven by the rapid integration of digital technologies, where cloud computing has emerged as one of the most dominant innovations reshaping business operations over the past decade. The expansion of the global cloud market from approximately US$109 billion in 2012 to US$246.8 billion in 2017 reflects not only technological advancement but also a structural shift in how organizations manage information systems and financial processes, particularly as firms transition from hardware-based infrastructures toward flexible, scalable, and cost-efficient cloud environments. This transition has enabled the emergence of cloud accounting as a critical component of digital financial ecosystems, offering real-time accessibility, reduced operational costs, and virtually unlimited scalability, which collectively enhance organizational agility and responsiveness in increasingly competitive markets (Yoon, 2020; Permana & Hadi, 2025).

At the same time, the integration of digital technologies into accounting practices has been closely associated with broader transformations in sustainability and accountability frameworks, indicating that cloud adoption is not merely a technical upgrade but part of a deeper reconfiguration of accounting systems within global digital economies (Petcu et al., 2024). However, the expansion of cloud-based systems is accompanied by heightened exposure to cybersecurity vulnerabilities, creating a complex landscape in which innovation and risk are inherently intertwined (Kumar et al., 2025). Prior research has consistently demonstrated that cloud-based accounting systems contribute to improved

financial reporting quality, enhanced efficiency, and streamlined data management processes, particularly through automation and real-time data integration (Adebimpe & Lola, 2024; Alagbe & Yinus, 2025; Apoorva & Tarachand, 2025).

In the context of small and medium-sized enterprises (SMEs), cloud computing has been identified as a critical enabler of accounting informatization, facilitating the digitalization and integration of financial information in ways that significantly improve operational flexibility and decision-making capacity (Meng, 2022). Empirical studies further indicate that cloud adoption decisions are shaped by a combination of perceived benefits, organizational readiness, and external environmental pressures, suggesting that adoption is a multifaceted process rather than a purely technological choice (Priyadarshinee et al., 2017). More recent findings reinforce the strategic importance of cloud computing as a driver of organizational performance and long-term digital transformation, while also highlighting its role in strengthening financial control systems and data-driven decision-making practices (Reis et al., 2025; Nguyen et al., 2025). Within this framework, the perceived value of cloud accounting is closely linked to its capacity to enhance transparency, accessibility, and efficiency, particularly in resource-constrained environments such as SMEs (Putri et al., 2025).

Despite these documented benefits, empirical evidence reveals that the adoption of cloud accounting has been slower than anticipated, suggesting the presence of underlying barriers that extend beyond technological capability. Industry reports indicate that early adoption rates were relatively low, with only 12% of firms in Australia and New Zealand adopting cloud accounting services as of 2013, while less than 30% of accountants and business owners expressed willingness to migrate their accounting processes to cloud environments (Dimitriu & Matei, 2015; Qoriah, 2025). This reluctance reflects deeper concerns regarding data security, privacy, and system reliability, which continue to shape user perceptions and decision-making processes. Existing studies highlight that trust in digital accounting systems is a critical determinant of adoption, yet this trust is often undermined by uncertainties related to cybersecurity risks and the perceived vulnerability of cloud infrastructures (Abad-Segura et al., 2024). At the same time, research on cloud adoption trends tends to emphasize technological and economic benefits while insufficiently addressing the psychological and risk-related dimensions that influence professional judgment, thereby creating a gap in understanding the full complexity of adoption behavior (Hasas & Samadzai, 2025).

The persistence of cybersecurity concerns further complicates this landscape, as the increasing prevalence of cybercrime continues to challenge the reliability of cloud-based systems. Reports indicate a rise in cybercrime incidents from 29% in 2018 to 35% in 2020, with significant impacts observed across multiple industries, including financial services, manufacturing, technology, and public sectors, underscoring the systemic nature of digital risk in contemporary economies. Cybersecurity threats in cloud environments are multifaceted, encompassing risks to data confidentiality, integrity, and availability, which collectively undermine the foundational principles of accounting information systems (Cebula & Young, 2010; Nawrocki et al., 2021). Within the accounting domain, the need for robust security mechanisms has become increasingly critical, as cloud-based systems handle highly sensitive financial data that are attractive targets for cyberattacks (Sanusi et al., 2025). Furthermore, limited cybersecurity awareness among practitioners, particularly in SMEs, exacerbates these risks by reducing the effectiveness of protective measures and hindering the successful implementation of cloud accounting systems (Rianto et al., 2025; Zureigat et al., 2025).

These unresolved tensions between innovation and risk highlight the urgent need for a more integrative analytical framework that captures the dynamic interplay between technological advancement and cybersecurity concerns in accounting practice. Existing literature remains fragmented, often treating the benefits of cloud computing and the risks of cybersecurity as separate domains of inquiry, which limits its capacity to explain how professionals navigate these competing considerations in real-world contexts. The growing complexity of digital ecosystems, combined with the increasing responsibility of accountants as stewards of financial data, necessitates a deeper exploration of how adoption decisions are shaped by both opportunity and risk. Addressing this gap requires not only theoretical integration but also methodological approaches capable of capturing the subjective and contextual dimensions of professional experience.

In this regard, systematic and rigorous synthesis of existing knowledge, guided by established frameworks such as PRISMA, becomes essential for ensuring the transparency and credibility of

scholarly inquiry (Page et al., 2021), while qualitative analytical approaches such as thematic analysis offer valuable tools for uncovering the underlying patterns of meaning in practitioners' perspectives (Braun & Clarke, 2006). This study aims to examine how accountants balance the pursuit of innovation with cybersecurity concerns in the adoption of cloud accounting systems, with a particular focus on identifying the key factors that shape their perceptions and decision-making processes. It seeks to contribute to the literature by developing a more comprehensive conceptual understanding of the interaction between technological benefits and perceived risks, while also advancing methodological approaches that capture the complexity of professional judgment in digital transformation contexts.

RESEARCH METHODS

This study employs an empirical qualitative research design to examine how accountants balance cybersecurity concerns in the adoption of cloud accounting systems. The population consists of 4,427 intermediate members of the Indonesian Institute of Accountants (Ikatan Akuntan Indonesia) in Jakarta and Bandung, representing professionals with diverse academic qualifications and varying levels of certification and engagement with accounting practices. A purposive sampling technique is applied to select participants who possess relevant experience or exposure to digital accounting technologies, ensuring the depth and relevance of the data. Primary data are collected through focus group discussions and in-depth semi-structured interviews, enabling the exploration of both individual perceptions and collective dynamics. The main construct, cybersecurity anxiety, is operationalized through an interview instrument developed based on the cybersecurity risk taxonomy proposed by Cebula and Young (2010), which categorizes risks into four domains: human actions, system and technological failures, internal process failures, and external events, each further specified into detailed sub-indicators to guide systematic data collection.

Data analysis is conducted using thematic analysis to identify patterns, relationships, and underlying meanings within participants' responses, following an iterative process of open coding, axial coding, and selective coding to generate comprehensive themes. The analytical process emphasizes interpretive depth while maintaining methodological rigor through triangulation of data sources, comparison between focus group and interview findings, and member checking to ensure the validity of interpretations. An audit trail is maintained to document the analytical decisions and enhance transparency and dependability. Although the study does not employ statistical or econometric techniques, the robustness of the findings is ensured through adherence to qualitative research standards, including credibility, confirmability, and consistency, thereby providing a reliable and nuanced understanding of how accountants negotiate the tension between technological innovation and cybersecurity risk in cloud accounting adoption.

RESULTS AND DISCUSSION

Cybersecurity Anxiety and Risk Perception in Cloud Accounting Adoption

The empirical findings reveal that cybersecurity anxiety constitutes a central cognitive filter through which accountants evaluate the feasibility of cloud accounting adoption, reflecting a multidimensional perception of risk shaped by both technical knowledge and professional responsibility. Participants consistently articulated concerns related to data confidentiality, system integrity, and service reliability, which align with the operational risk taxonomy proposed by Cebula and Young (2010). These concerns are not merely abstract but embedded in daily accounting practices where financial data sensitivity elevates perceived exposure to cyber threats. The interpretive patterns suggest that cybersecurity anxiety operates as a moderating force that reshapes perceived usefulness into a conditional rather than absolute determinant of adoption.

Qualitative evidence from interviews indicates that human-related risks, particularly inadvertent errors and insufficient security awareness, dominate the discourse among participants, revealing a persistent vulnerability within organizational routines. Respondents emphasized that weak password practices, credential sharing, and limited understanding of cloud security protocols increase exposure to unauthorized access, which reinforces perceived risk severity. This observation resonates with prior findings that highlight the critical role of human factors in cybersecurity resilience (Rianto et al., 2025). The data further indicate that even technologically advanced systems remain susceptible to risk when user behavior is not aligned with security standards. The thematic coding also identifies system and technological failures as a significant dimension influencing cybersecurity anxiety, particularly in

relation to software bugs, integration failures, and unexpected downtime. Participants frequently associated cloud environments with reduced direct control over system infrastructure, which contributes to a sense of uncertainty regarding system dependability. This perception reflects broader concerns in cloud optimization literature, where system adaptability must be balanced with robust security mechanisms (Nawrocki et al., 2021). The resulting tension illustrates that technological sophistication alone does not guarantee user confidence in cloud-based systems.

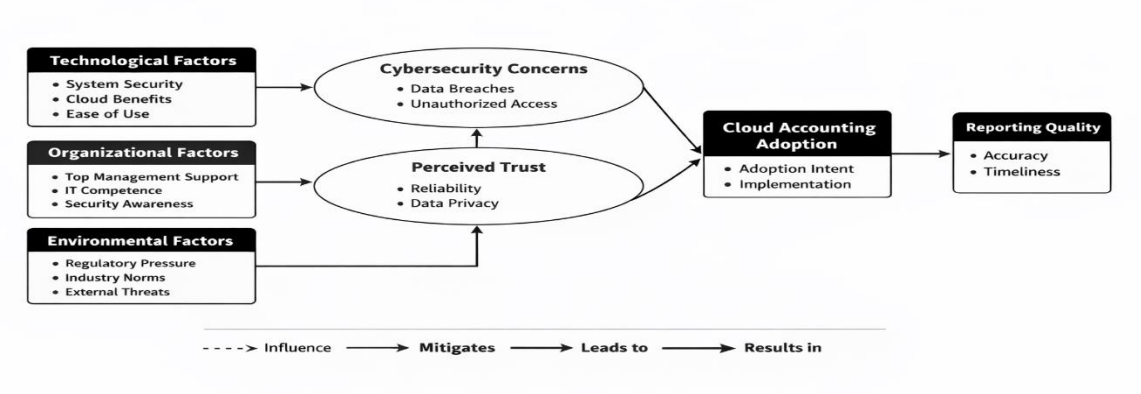

Figure 1. Conceptual Framework of the Study

Internal process failures emerge as another critical theme, particularly regarding inadequate control mechanisms and poorly designed operational procedures that fail to align with cloud-based workflows. Participants noted that traditional accounting controls are often insufficiently adapted to cloud environments, leading to gaps in monitoring and risk mitigation. Such findings reinforce the argument that digital transformation requires not only technological change but also organizational restructuring of internal processes (Meng, 2022). The absence of updated procedural frameworks amplifies perceived vulnerability and contributes to resistance toward adoption.

External risk factors, including regulatory uncertainty and dependence on third-party service providers, further intensify cybersecurity concerns among accountants. Respondents expressed skepticism regarding the legal accountability of cloud service providers in the event of data breaches, highlighting the perceived asymmetry of control between users and vendors. This aligns with broader discussions on environmental pressures influencing cloud adoption decisions (Priyadarshinee et al., 2017). The interplay between external uncertainty and internal preparedness shapes a complex risk environment that influences adoption behavior. In the middle of this analytical discussion, the distribution of perceived cybersecurity risks across thematic categories is summarized in Table 1, which provides a structured representation of participant responses and coding frequency.

Table 1. Distribution of Cybersecurity Risk Perceptions Among Participants

Risk Category	Frequency	Dominant Sub-Issues
Human Actions	High	Inadvertent errors, weak credentials
System & Technology Failures	Medium	Downtime, software bugs
Internal Process Failures	High	Weak controls, poor procedures
External Events	Medium	Regulatory uncertainty, vendors

The data in Table 1 demonstrate that human actions and internal process failures are the most salient sources of cybersecurity anxiety, indicating that risk perception is strongly influenced by organizational and behavioral dimensions rather than purely technical factors. This distribution suggests that improving cybersecurity awareness and internal governance structures may yield greater impact than solely enhancing technological infrastructure. The findings support the argument that cybersecurity risk is socially constructed through professional experience and organizational context (Sanusi et al., 2025). The table reinforces the need for a holistic approach to risk management in cloud adoption. Further analysis reveals that cybersecurity anxiety is not uniform across participants but varies according to professional experience and exposure to digital systems. Accountants with prior

experience in cloud environments tend to exhibit more nuanced risk assessments, distinguishing between manageable and critical threats. This observation aligns with studies emphasizing the role of experiential learning in shaping technology adoption behavior (Reis et al., 2025).

Variations in perception indicate that risk is interpreted through both cognitive and experiential lenses. The findings also indicate that cybersecurity anxiety does not necessarily lead to outright rejection of cloud accounting but instead encourages more cautious and selective adoption strategies. Participants described adopting hybrid systems or implementing additional security measures as a way to mitigate perceived risks while still leveraging technological benefits. This behavior reflects a balancing mechanism rather than a binary decision-making process, supporting the notion that adoption is iterative and adaptive (Nguyen et al., 2025). Such strategies illustrate how professionals actively negotiate the tension between innovation and risk.

Interpretively, cybersecurity anxiety can be understood as a rational response to structural uncertainties inherent in cloud computing environments, rather than as a barrier rooted in resistance to change. The findings suggest that accountants are not inherently risk-averse but are engaged in a process of risk calibration that integrates professional judgment and contextual knowledge. This perspective aligns with the view that digital transformation requires alignment between technological capability and user trust (Putri et al., 2025). The empirical evidence highlights the need to reconceptualize cybersecurity concerns as an integral component of innovation adoption rather than an external obstacle.

Perceived Trust as a Mediating Mechanism in Cloud Accounting Adoption

The findings indicate that perceived trust operates as a pivotal mediating construct that shapes how accountants reconcile cybersecurity concerns with the perceived benefits of cloud accounting systems. Participants consistently framed trust not as an inherent attribute of technology but as a contingent evaluation influenced by system reliability, data protection assurances, and institutional credibility. This aligns with the broader understanding that trust in digital systems emerges through repeated validation of system performance and governance structures rather than initial technological appeal (Sanusi et al., 2025). The empirical evidence suggests that trust functions as a cognitive bridge that transforms risk awareness into conditional acceptance rather than outright rejection.

Qualitative responses reveal that reliability constitutes a primary dimension of perceived trust, particularly in relation to system uptime, data consistency, and operational continuity. Accountants emphasized that consistent system performance reduces uncertainty and fosters confidence in cloud-based environments, even in the presence of known cybersecurity risks. This observation reflects the argument that perceived system reliability significantly influences technology adoption decisions in professional contexts (Sarker, 2025). The findings suggest that reliability serves as a stabilizing factor that mitigates the psychological impact of perceived vulnerabilities. Data privacy emerges as another critical component shaping trust, especially given the sensitive nature of financial information handled by accountants. Participants expressed concerns regarding data ownership, storage location, and potential unauthorized access by third parties, which directly influence their willingness to engage with cloud systems. These concerns are consistent with prior studies highlighting the centrality of privacy assurance in digital accounting environments (Wahhab et al., 2024).

The data indicate that trust is strengthened when clear data governance policies and encryption mechanisms are communicated effectively to users. The role of organizational support is also evident in shaping perceived trust, particularly through the provision of training, security protocols, and institutional safeguards. Participants noted that organizations with structured cybersecurity policies and continuous professional development programs tend to foster higher levels of trust among employees. This finding supports the notion that organizational readiness is a key determinant of successful cloud adoption (Priyadarshinee et al., 2017). Trust is thus constructed not only through technological features but also through institutional reinforcement and capacity building.

Participants highlighted the importance of external validation, such as compliance with regulatory standards and certifications provided by cloud service providers. These external signals serve as proxies for system credibility and influence trust formation, especially in environments where direct technical evaluation is not feasible. This aligns with the literature emphasizing the role of environmental and institutional factors in shaping technology adoption behavior (Reis et al., 2025). The presence of recognized certifications reduces perceived ambiguity and enhances confidence in cloud services. To illustrate the multidimensional structure of perceived trust, Table 2 presents the thematic distribution of

trust-related factors identified in the data, along with their relative prominence across participant responses.

Table 2. Dimensions of Perceived Trust in Cloud Accounting Adoption

Trust Dimension	Frequency	Key Indicators
System Reliability	High	Uptime, consistency, performance
Data Privacy	High	Encryption, access control, ownership
Organizational Support	Medium	Training, policies, internal controls
External Assurance	Medium	Certifications, regulatory compliance

The data in Table 2 demonstrate that system reliability and data privacy are the most dominant dimensions influencing trust, indicating that technical and informational assurances are prioritized by accounting professionals. Organizational and external factors, while slightly less prominent, still play a significant role in reinforcing trust perceptions. This distribution suggests that trust is constructed through a layered interaction between technological performance and institutional legitimacy (Putri et al., 2025). The findings reinforce the argument that trust is a multidimensional construct that cannot be reduced to a single determinant. The analysis further reveals that perceived trust moderates the relationship between cybersecurity anxiety and adoption intention, effectively transforming risk into a manageable consideration rather than a prohibitive barrier. Participants who reported higher levels of trust demonstrated greater willingness to adopt cloud accounting systems despite acknowledging potential risks. This pattern supports the conceptualization of trust as a mitigating mechanism that reduces perceived uncertainty in digital environments (Nguyen et al., 2025).

The findings suggest that enhancing trust can offset the negative effects of cybersecurity concerns. In addition, trust appears to be dynamically constructed through experience, with repeated positive interactions with cloud systems strengthening confidence over time. Participants with prior exposure to cloud technologies exhibited more balanced evaluations, integrating both benefits and risks into their decision-making processes. This observation aligns with the view that experiential learning plays a critical role in shaping technology acceptance (Meng, 2022). Trust, therefore, evolves as a function of both cognitive assessment and practical engagement. The findings also indicate that low levels of trust amplify the perceived severity of cybersecurity risks, leading to heightened resistance or delayed adoption decisions. Participants lacking confidence in system security or provider reliability tended to emphasize worst-case scenarios, which influenced their overall evaluation of cloud technologies. This behavior reflects the cognitive bias toward risk amplification in uncertain environments (Nawrocki et al., 2021).

The interplay between trust and risk perception highlights the importance of addressing both dimensions simultaneously in adoption strategies. From an interpretive perspective, perceived trust can be understood as a critical balancing mechanism that enables accountants to navigate the inherent tension between innovation and risk in cloud accounting adoption. The empirical evidence suggests that trust does not eliminate cybersecurity concerns but reframes them within a manageable and controllable context. This nuanced understanding contributes to the broader discourse on digital transformation by emphasizing the role of psychological and institutional factors in shaping professional behavior. The findings underscore the necessity of integrating trust-building strategies into technological implementation to achieve sustainable adoption outcomes.

Cloud Accounting Adoption Outcomes and Implications for Financial Reporting Quality

The findings demonstrate that cloud accounting adoption among accountants is not merely a technological transition but a consequential process that reshapes financial reporting practices and organizational performance. Participants reported that the adoption process is often gradual and contingent upon the successful negotiation of cybersecurity concerns and trust formation. This supports the argument that technology adoption is an iterative process influenced by both perceived benefits and risk considerations (Nguyen et al., 2025). The empirical evidence indicates that adoption outcomes are closely tied to how effectively organizations balance innovation with risk management. A dominant theme emerging from the data is the perceived improvement in financial reporting efficiency, particularly in terms of timeliness and data accessibility. Participants emphasized that cloud systems

enable real-time data updates and facilitate faster reporting cycles, which enhance decision-making processes within organizations. These findings are consistent with prior research indicating that cloud accounting systems significantly improve reporting efficiency through automation and integration (Sarker, 2025).

The qualitative insights suggest that efficiency gains are among the most tangible benefits experienced by users. Accuracy in financial reporting also emerges as a critical outcome associated with cloud accounting adoption, driven by reduced manual intervention and enhanced data consistency. Respondents noted that automated processes minimize human error and improve the reliability of financial information, which is essential for maintaining professional standards. This observation aligns with studies highlighting the positive relationship between cloud accounting and reporting quality (Wahhab et al., 2024). The findings reinforce the notion that technological integration contributes to improved data integrity. However, the data also reveal that these positive outcomes are conditional upon the effectiveness of cybersecurity measures embedded within the system. Participants expressed that without adequate security controls, the benefits of efficiency and accuracy could be undermined by risks such as data breaches and unauthorized access. This reflects the broader concern that technological advantages must be supported by robust security frameworks to ensure sustainable adoption (Sanusi et al., 2025).

The interplay between performance outcomes and risk mitigation remains a central consideration in adoption decisions. Another important finding relates to the role of cloud accounting in enhancing financial transparency and accountability within organizations. Participants indicated that centralized data storage and standardized reporting processes improve auditability and facilitate compliance with regulatory requirements. This aligns with the argument that digital accounting systems contribute to greater organizational transparency and governance (Putri et al., 2025). The improved visibility of financial data strengthens stakeholder confidence and supports strategic decision-making. To further illustrate the perceived outcomes of cloud accounting adoption, Table 3 presents a summary of key reporting quality dimensions identified through thematic analysis, along with their relative prominence among participants.

Table 3. Perceived Impact of Cloud Accounting on Financial Reporting Quality

Reporting Dimension	Frequency	Key Indicators
Timeliness	High	Real-time reporting, faster cycles
Accuracy	High	Reduced errors, data consistency
Transparency	Medium	Auditability, standardized reports
Accessibility	High	Remote access, data availability

The data in Table 3 indicate that timeliness, accuracy, and accessibility are the most prominent benefits perceived by participants, suggesting that operational efficiency is a primary driver of adoption outcomes. Transparency, while slightly less emphasized, remains an important dimension that contributes to improved governance and accountability. This distribution reflects the multifaceted impact of cloud accounting on reporting quality, extending beyond technical efficiency to include institutional implications (Meng, 2022). The findings highlight the interconnected nature of performance outcomes in digital accounting systems. Despite these advantages, participants also reported challenges related to system dependency and the need for continuous monitoring of cloud service performance. The reliance on external service providers introduces new forms of risk, particularly in relation to service disruptions and data management practices. This observation aligns with research emphasizing the importance of adaptive system optimization in cloud environments (Nawrocki et al., 2021).

The findings suggest that organizations must develop strategies to manage dependency risks effectively. The role of cybersecurity awareness is further reinforced in shaping the quality of adoption outcomes, as participants with higher levels of awareness reported more positive experiences with cloud

accounting systems. These individuals demonstrated greater ability to implement protective measures and respond to potential threats, thereby enhancing system reliability and performance. This supports the argument that cybersecurity literacy is a critical determinant of successful technology implementation (Rianto et al., 2025). The findings indicate that human capital plays a significant role in maximizing the benefits of cloud adoption. Environmental and regulatory factors also influence the extent to which cloud accounting adoption translates into improved reporting quality. Participants highlighted the importance of supportive regulatory frameworks and industry standards in ensuring secure and effective system implementation. This aligns with the literature suggesting that external pressures and institutional environments shape technology adoption outcomes (Priyadarshinee et al., 2017).

The interaction between internal capabilities and external conditions determines the overall success of adoption. From an interpretive standpoint, the findings suggest that cloud accounting adoption outcomes are best understood as the result of a dynamic equilibrium between innovation benefits and cybersecurity risks. The empirical evidence indicates that while cloud systems offer substantial improvements in reporting quality, these benefits are contingent upon the presence of adequate security measures, organizational readiness, and user competence. This perspective contributes to the broader discourse on digital transformation by emphasizing the conditional nature of technological benefits. The study highlights the need for integrated strategies that align technological innovation with risk management to achieve sustainable improvements in financial reporting quality.

CONCLUSION

This study concludes that the adoption of cloud accounting represents a complex and dynamic process shaped by the interaction between technological innovation, cybersecurity concerns, and trust formation among accountants. The findings reveal that cybersecurity anxiety plays a significant role in influencing adoption decisions, particularly when accountants perceive risks related to data breaches, system vulnerabilities, and external threats. However, such concerns do not necessarily inhibit adoption; rather, they encourage more cautious and selective engagement with cloud technologies. Trust emerges as a critical mediating factor that enables accountants to reconcile perceived risks with the potential benefits of digital transformation. Furthermore, the study demonstrates that cloud accounting adoption leads to notable improvements in financial reporting quality, particularly in terms of timeliness, accuracy, and accessibility of financial information. These benefits, however, are conditional upon the effectiveness of cybersecurity measures, user competence, and organizational readiness. The results indicate that successful adoption is not solely determined by technological capabilities but also by the ability of individuals and organizations to manage risks and build confidence in digital systems. Ultimately, this study highlights the importance of integrating cybersecurity awareness, trust-building mechanisms, and institutional support to ensure that cloud accounting adoption contributes sustainably to enhanced financial reporting practices.

REFERENCES

Abad-Segura, E., et al. (2024). Secure perception of accounting systems with digital technologies. *Journal of Open Innovation*, 100264.

Adebimpe, O. I., & Lola, A. O. (2024). Cloud-based accounting information systems and reporting quality. *Journal of Economics and Finance Management Studies*, 7(4).

Alagbe, E. A., & Yinus, S. O. (2025). Cloud accounting practice and financial reporting quality. *International Journal of Multidisciplinary Research and Analysis*, 8(4).

Apoorva, G., & Tarachand, A. M. (2025). Impact of cloud-based accounting on financial reporting efficiency. *International Journal of Research and Technology*, 13(2).

Braun, V., & Clarke, V. (2006/updated usage widely 2016–2021). Using thematic analysis in psychology. *Qualitative Research in Psychology*.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Hasas, A., & Samadzai, A. W. (2025). Adoption of cloud-based accounting software in enterprises. *Journal of Advanced Computer Knowledge and Algorithms*, 2(4).

Kumar, P., et al. (2025). Cybersecurity challenges and opportunities in cloud transformation. *Computers & Security*, 151, 104339. https://doi.org/10.1016/j.cose.2025.104339

Meng, L. (2022). Cloud computing and accounting informatization in SMEs. *Mobile Information Systems*, 2022, 1–13.

Nawrocki, P., et al. (2021). Adaptive cloud computing optimization considering security aspects. *Concurrency and Computation: Practice and Experience*, 33(18), e6070.

Nguyen, G. P., Hoang, T. T., & Tran, H. N. B. (2025). The impact of cloud computing technology on cloud accounting adoption and financial management of businesses. *Humanities and Social Sciences Communications*, 12, 851. https://doi.org/10.1057/s41599-025-05190-3

Page, M. J., et al. (2021). PRISMA 2020 statement. *BMJ*, n71.

Permana, N., & Hadi, S. P. (2025). Systematic analysis of cloud adoption trends.

Petcu, M. A., et al. (2024). Integrating digital technologies in sustainability accounting.

Priyadarshinee, P., et al. (2017). Cloud computing adoption in SMEs: Literature review. *International Journal of Information Management*, 36(4), 503–514.

Putri, E., et al. (2025). The value of cloud accounting for MSMEs: TOE framework perspective. *Cogent Business & Management*, 12(1).

Qoriah, D. (2025). Adoption of cloud accounting: Opportunities and barriers.

Reis, A., Fraga, C., & Gouveia, A. J. (2025). Cloud computing adoption as IT strategy in organizations: A systematic review. *Procedia Computer Science*, 256, 122–129.

Rianto, R., Aulia, T. Z., & Sudarmanto, E. (2025). Cloud accounting implementation and cybersecurity awareness in MSMEs. *Yudishtira Journal of Finance and Strategy*, 5(3), 616–641.

Sanusi, I., Sanusi, A. R., Shamwill, A. K., & Yinusa, S. (2025). Evaluation of cloud-based computing in security accounting information system. *World Journal of Advanced Research and Reviews*, 25(3), 1073–1086. https://doi.org/10.30574/wjarr.2025.25.3.0734

Sarker, J. (2025). Cloud accounting system and financial reporting efficiency of SMEs. *International Journal of Science and Business*, 48(1), 75–91.

Wahhab, A. M. A., et al. (2024). Cloud accounting implementation and financial reporting quality. *Financial and Credit Activity*, 54, 146–159.

Yoon, S. (2020). Cloud computing benefits in financial accounting systems. *Information*, 11(2), 92.

Zureigat, B. N., et al. (2025). Cybersecurity awareness and digital accounting systems performance. *Economic and Organizational Issues*, 375–396. https://doi.org/10.2478/eoik-2025-0070