ISSN (Print): 1060-6076
ISSN (Online): Applied

The Journal of African Development
2026; Vol 7: Issue 1
https://www.afea-jad.com/

Quantum-Secured Accounting Information Systems: A New Paradigm for Financial Data Integrity and Assurance

Dr. Fatemabibi Abubaker Salehbhai [1]

[1]Assistant Professor, School of Liberal Arts and Management Studies P P Savani University, Kosamba, Surat – 394125, Gujarat, India

Email ID : sfa_714@yahoo.com

Cite This Paper as: Dr. Fatemabibi Abubaker Salehbhai (2026) Quantum-Secured Accounting Information Systems: A New Paradigm for Financial Data Integrity and Assurance. The Journal of African Development l, Vol.7, No.1, 700-706

KEYWORDS

Accounting Information System, Quantum – Secured, Integrity, Challenges

ABSTRACT

The complex of processes involved yields Accounting Information Systems (AIS), whereby financial data is recorded, processed, and stored that has important implications not only for decision-making, but also regulatory compliance and stakeholder assurance. While accounting practices have moved towards a digital transformation, accounting systems are increasingly susceptible to advanced cyber threats, data breaches, and financial manipulation. In this paper, a new paradigm of Quantum-Secured Accounting Information Systems (AIS) is proposed as a preventive framework aimed at dealing with the novelty of cybersecurity threats posed by quantum computing. It discusses and critiques how classical crypto-based AIS are open to exposures of some very serious threats and then outlines the ideas for a quantum security aware framework addressing financial data integrity, audit reliability, confidence by stakeholders. By compiling existing interdisciplinary literature, spanning accounting through cybersecurity to quantum technology, the paper constructs a multi-layered architecture of AIS secured with quantum technologies that includes data protection, access control and audit compliance. The paper further relates the implications of these systems for financial reporting, auditing and corporate governance while identifying primary challenges to adoption in terms of infrastructure costs and skills shortages are identified as well as legacy system integration challenges and a lack of quantum standards specific to the accounting profession. Finally, it provides guidelines for future research to empirically test organizational readiness and the impacts of classical vs. quantum secured AIS on audit quality and preventing fraud especially in developing countries. This research contributes to AIS literature by proposing a future-oriented framework that readies accounting systems for the post-quantum era.

1. INTRODUCTION

Accounting Information System (AIS) refers to tools and systems of the processing, storage, and reporting of accounting information. The rapid digital evolution of accounting systems has led to an increased reliance on cloud-based accounting systems, enterprise resource planning (ERP) systems, and real-time financial reporting systems. Although these developments have increased the efficiency and accessibility of accounting systems, they have also increased the vulnerability of accounting systems to complex cyber-attacks, data breaches, and financial fraud. The security of Accounting Information Systems has traditionally relied on classical cryptographic methods to guarantee the confidentiality, integrity, and availability of financial information. The appearance of quantum computing, however, poses a basic challenge to these classical security methods. Quantum computers have the potential to break widely used encryption algorithms, thus making sensitive accounting information vulnerable to new risks. The emergence of quantum computing poses a significant challenge to these conventional security mechanisms, as quantum computers possess the capability to undermine widely used encryption algorithms, thereby exposing sensitive accounting data and audit trails to unprecedented risks (Shadan, Huma, & Islam, 2025; Kasheem, Shalghoum, & Abdullah, 2025). Quantum security solutions, such as post-quantum cryptography and quantum-based authentication mechanisms, offer novel methods to protect financial data against both current and future cyber threats. While quantum security has begun to garner attention in fields such as banking, cybersecurity, and financial technology, its application within the domain of accounting information systems remains largely unexplored. While the application of quantum security has gained attention in

banking and financial technology sectors, its integration within accounting information systems remains largely unexplored (Lazirko, 2023; Mulla, 2025). Given the increasing reliance on automated accounting processes and continuous auditing, the absence of quantum-resilient security frameworks in AIS threatens data integrity, audit assurance, and corporate governance in the long term (Ekici, 2025; Bell, Mitchell, & Barrett, 2020). Existing accounting literature has predominantly concentrated on internal controls, auditing standards, and classical cybersecurity measures, leaving a substantial research gap concerning the integration of quantum security into AIS. This gap is particularly critical given the increasing reliance on automated accounting processes, continuous auditing, and digital financial reporting. The absence of quantum-resilient security frameworks in AIS may compromise data integrity, audit assurance, and corporate governance in the long term. As accounting systems evolve into strategic information assets, ensuring their resilience against quantum-era threats becomes not only a technological necessity but also an accounting and governance imperative. In this context, the present study aims to conceptualize a new paradigm of Quantum-Secured Accounting Information Systems. By synthesizing insights from accounting information systems literature, cybersecurity research, and emerging quantum technologies, this paper develops a conceptual framework that elucidates how quantum security can be integrated into AIS to enhance financial data integrity, audit reliability, and stakeholder trust. The study contributes to the accounting literature by extending AIS research beyond traditional cybersecurity approaches and offering a forward-looking framework that prepares accounting systems for the post-quantum era.

LITERATURE REVIEW

Shadan, Huma, and Islam (2025) carried out a review of the transformative effect of quantum computing on the improvement of cybersecurity in accounting and finance. The purpose of the review was to investigate the potential of quantum algorithms and Quantum Key Distribution (QKD) to overcome the shortcomings of classical computing and improve the level of cybersecurity in accounting. The study was carried out using secondary data, which was obtained from a comprehensive review of existing literature, and was analysed using the PSALSAR systematic review approach. The results of the study showed that the existing level of cybersecurity in accounting was susceptible to quantum attacks and that classical encryption methods could become obsolete with the development of quantum capabilities. The conclusion of the study was that the use of quantum-resistant cryptographic algorithms and QKD is necessary for the future-proofing of accounting and finance systems because these technologies have the potential to greatly reduce data breaches, unauthorized access, and improve encryption beyond classical methods.

Mulla (2025), investigated the use of quantum computing and its ability to revolutionize accounting and finance processes. The research aimed to investigate how quantum accounting could improve financial data processing, increase the accuracy of auditing, improve risk analysis, and increase data security by leveraging quantum technology. The research was conducted using secondary data, which was collected from existing literature, theories, and previous research studies on quantum computing and its financial applications. It is concluded that the quantum algorithm, such as Grover's search algorithm and quantum machine learning, made it possible to process complex financial data efficiently compared to existing computing processes. The research also highlighted some challenges that prevented the effective implementation of quantum accounting, such as the limitations of hardware, lack of qualified personnel, and regulatory issues. The conclusion highlighted that the early adoption of quantum technology could create a competitive advantage in terms of speed, accuracy, and security for financial institutions, but it is important to address technological, human resource, and regulatory issues to fully exploit the benefits of quantum accounting.

Lazirko (2023), investigated the possible implications of quantum technology on accounting information systems and business operations. The aim of the study was to investigate the risks related to quantum computing, evaluate the new quantum-resistant encryption algorithms, and determine the effects of quantum standards on the efficiency, speed, and security of business operations. The study was based on secondary data, which included an analytical review of existing standards, frameworks, and literature on quantum technology and cybersecurity best practices. The results of the study showed that different organizations were actively engaged in the development of quantum standards, and there were obvious differences, similarities, and limitations between the American and European approaches. The study also indicated that it was important for organizations to understand the relationship between quantum technology and standard-setting organizations in order to improve cybersecurity and ensure the integrity of business operations. The conclusion of the study reiterated that organizations should adopt best practices and strategies that were in line with the evolving quantum standards in order to effectively address cyber threats and prepare for the challenges posed by the emergence of quantum computing capabilities.

Kasheem, Shalghoum, and Abdullah (2025), investigated the impact of quantum computing on Accounting Information Systems by focusing on the challenges of processing speed, computational capability, and data security. The research was conducted to analyze the opportunities and challenges of implementing quantum computing in AIS, and the study was supported by secondary data. The results revealed that quantum algorithms enhanced data processing, financial modeling, and encryption security, but the conclusion highlighted that hardware limitations, threats of cryptographic disruption, and a lack of professional knowledge were major hurdles in implementing quantum computing.

Demski, FitzGerald, Ijiri, and Lin (2009), continued from their previous research to explore the concept of topological quantum computation and its conceptual applicability to accounting information systems. The research was conceptual and theoretical in nature and supported by previous research in the field of quantum computation and accounting theory. The

results of the research revealed that topological quantum computation provided protection against imprecision and decoherence and also emphasized the qualitative aspects of control error frequencies, as opposed to the traditional quantitative approach in accounting. The conclusion drawn from the research was that the incorporation of topological concepts into accounting theory expanded the scope of analysis and provided new avenues for interdisciplinary research between quantum information science and accounting systems.

Bell, Mitchell, and Barrett (2020), examined the impact of next-generation Accounting Information Systems on organizational efficiency by applying the principles of quantum-inspired optimization algorithms to traditional systems analysis. The research work focused on the development and validation of a multi-dimensional framework for evaluating financial reporting efficiency and explored the application of quantum-inspired principles for optimizing financial reporting processes. The research work used a hybrid approach, which combined agent-based computational simulation with empirical validation in three industries. The results showed that quantum-inspired AIS designs resulted in a 42% reduction in financial closing times, a 67% decrease in errors during reconciliation, and more than 58% reduction in cognitive load. The research work concluded that the efficiency of Accounting Information Systems is not just dependent on processing speed but also on the overall integration of human and system perspectives, and that future AIS designs need to focus on cognitive optimization and system architecture for making revolutionary changes in financial reporting.

Ekici (2025), investigated the interdisciplinary impacts of quantum computing technologies on accounting and finance. The research was intended to analyze how quantum technologies might change financial applications, accounting information systems, leadership styles, and decision-making models. The research was grounded on secondary data obtained from a thorough review of recent scientific publications and official documents. The results showed that quantum algorithms offered great advantages in terms of speed and accuracy in derivative pricing, portfolio optimization, and risk management, but the current encryption techniques were susceptible to quantum attacks, requiring post-quantum cryptography. It was concluded that quantum technologies have the potential to revolutionize the accounting profession not only from a technical perspective but also from an ethical and structural point of view, implying that accounting professionals must be re-skilled to cope with the requirements of the new quantum age.

Fellingham & Schroeder (2006), examined the efficiency of double-entry processing of information based on the principles of quantum probability. The authors sought to show how quantum probabilities, which are distinct from classical probabilities because of quantum interference and entanglement, might improve performance evaluation in accounting information systems. The authors used theoretical and conceptual research to apply the principles of quantum probability to accounting information structures. The results showed that when quantum interference was combined with correlation or entanglement, double-entry processing resulted in a smaller and more efficient set of performance measures, enabling the performance of both agents to be assessed with the same information signal. The study showed that the compact information system was more incentive-efficient than the conventional method of evaluating each agent separately, thus illustrating the relevance of quantum principles in accounting information design.

Research Objectives

- To examine cybersecurity vulnerabilities in traditional Accounting Information Systems
- To explore the role of quantum security technologies in strengthening AIS
- To propose a conceptual framework for Quantum-Secured Accounting Information Systems
- To analyse implications for financial reporting, auditing, and corporate governance

Research Methodology

The study employs conceptual and qualitative research approach that builds on an extensive, interdisciplinary literature review. The research employs a methodical approach, systematically gathering and synthesizing secondary data from academic publications, industry reports, and technological overviews across the realms of accounting information systems, cybersecurity, and quantum technologies. Important sources may contain the fields of empirical studies, theoretical documentation and standard records concerning the classical-primarily based totally protection and quantum-safety paradigms in economic facts control. Based on this methodological approach, the paper is able to present a future-oriented and theory-driven structuring of quantum security ability in AIS as preparing the accounting discipline for post-quantum times.

- **Conceptual Framework: Quantum-Secured AIS**

Quantum-Secured AIS is a model of accounting information systems that integrates quantum cryptography and advanced cybersecurity mechanisms to make full protection for financial data. It highlights the application of quantum key distribution (QKD), secure encryption protocols, and decentralized validation methods to deter unauthorized access, data manipulation, and cyber-fraud in accounting records. The companies verifiable triple-entries system is a base for building of supreme secure and trust less financial reporting office in dynamic cybernetic environment, hyper-specialization and post-quantum era.

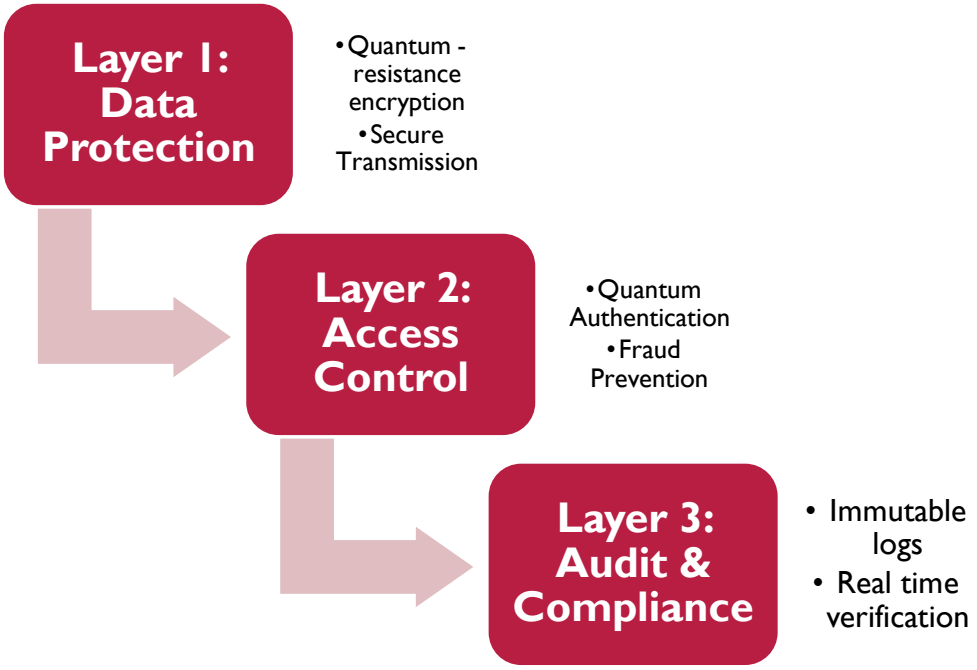
  - **Traditional AIS Components**

Data input is the first stage of a traditional Accounting Information System (AIS) and involves the collection and entry of financial data into the system. This includes source documents such as vouchers, invoices, receipts, purchase orders, payroll records, and transaction slips. These documents serve as primary evidence of business transactions and must be verified for accuracy and authenticity before entry. In modern organisations, data may be entered manually or captured automatically through scanning systems, electronic data interchange (EDI), or integrated business applications. The reliability of the entire AIS depends heavily on the accuracy, completeness, and timeliness of this input stage, as errors at this level can propagate throughout the system and affect financial reporting. Processing refers to the transformation of raw financial data into meaningful accounting information. Once transactions are entered, the system classifies, calculates, summarises, and records them according to accounting principles. This includes activities such as ledger posting, journal entries, trial balance preparation, cost allocation, and financial consolidation across departments or subsidiaries. Processing also involves applying accounting rules, validation checks, and automated calculations to ensure consistency and compliance with accounting standards. Efficient processing enhances decision-making by providing timely and structured financial insights while reducing manual effort and computational errors. Storage is the component where financial data is securely maintained for present and future use. Traditional AIS typically stores information in databases hosted on local servers, enterprise resource planning (ERP) systems, or cloud-based platforms. Storage systems must ensure data integrity, confidentiality, and availability, as accounting data is highly sensitive and subject to regulatory requirements. Proper storage mechanisms include backup systems, access controls, encryption, and audit trails to prevent data loss, unauthorised access, or manipulation. Well-structured storage also facilitates easy retrieval of historical financial information for audits, analysis, forecasting, and compliance reporting. Output represents the final stage of AIS, where processed information is presented in a usable format for stakeholders. Outputs include financial statements such as balance sheets, income statements, and cash flow statements, as well as management information system (MIS) reports, tax reports, budgets, and performance analyses. These reports support internal decision-making by managers and external reporting to investors, regulators, and auditors. The quality of AIS output depends on the accuracy of input data, effectiveness of processing, and reliability of storage systems. Well-designed outputs are clear, timely, relevant, and compliant with accounting standards, enabling organisations to monitor performance, ensure transparency, and maintain stakeholder confidence.

- **Quantum Security Layer**

Quantum-safe encryption refers to cryptographic techniques designed to remain secure even against attacks from quantum computers, which are capable of breaking many classical encryption systems. In an Accounting Information System (AIS), transaction data such as journal entries, payment records, invoices, and financial transfers must be protected from interception or manipulation. Quantum-safe algorithms—often called post-quantum cryptography—use complex mathematical structures that cannot be efficiently solved by quantum algorithms. By integrating these encryption methods into AIS, organisations can ensure that financial data remains confidential, tamper-proof, and resistant to future cyber threats, thereby strengthening trust in digital accounting environments. The second layer for quantum security is quantum authentication which enhances access control mechanisms by using quantum-based verification techniques to validate user identity. Unlike traditional password or token systems, quantum authentication can employ quantum keys or quantum signatures that are nearly impossible to forge due to the fundamental laws of quantum physics. In an AIS environment, this ensures that only authorised personnel—such as accountants, auditors, or administrators—can access sensitive financial systems. Such authentication reduces the risk of unauthorised access, identity spoofing, and insider threats, thereby improving system integrity and compliance with cybersecurity regulations. The last layer of is Quantum-secured audit trails. Audit trails record every transaction, modification, and access event within an accounting system, forming a crucial component for transparency, compliance, and forensic analysis. Quantum-secured audit trails apply quantum cryptographic methods to ensure that once records are created, they cannot be altered without detection. Techniques such as quantum hashing and entanglement-based verification make any tampering immediately evident. This ensures the immutability and reliability of audit logs, which is particularly important for regulatory reporting, fraud detection, and external audits. As a result, quantum-secured audit trails enhance the credibility of financial reporting and provide stronger assurance to stakeholders.

Architecture of Quantum-Secured AIS



- **Architecture of Quantum-Secured AIS**
  - **Layer 1: Data Protection**

Quantum-resistant encryption refers to cryptographic algorithms designed to withstand attacks from quantum computers, which could otherwise break traditional encryption methods. In an Accounting Information System (AIS), this ensures sensitive financial records such as ledgers, invoices, payroll data, and tax reports remain confidential and protected even in a future quantum computing environment. Quantum-secured communication uses advanced encryption protocols and quantum key distribution (QKD) principles to safeguard data while it is transmitted across networks. This prevents interception, tampering, or unauthorized access when financial data is shared between different organizational units, branches, or external stakeholders like auditors and regulators.

  - **Layer 2: Access Control**

Quantum authentication mechanisms rely on quantum cryptographic keys or quantum tokens that cannot be copied or forged due to the laws of quantum physics. This ensures that only authorized personnel—such as accountants, auditors, or financial managers—can access sensitive accounting systems and perform transactions or audits. Traditional systems depend on passwords, PINs, or access cards, which can be stolen or duplicated. Quantum-secured access systems remove these vulnerabilities by using unbreakable cryptographic verification, drastically reducing risks such as identity theft, insider fraud, and unauthorized financial manipulation.

  - **Layer 3: Audit & Compliance**

Quantum-secured audit logs create tamper-proof records of all financial activities and system access events. Once a transaction or change is recorded, it cannot be altered or deleted without detection, ensuring transparency, accountability, and strong forensic evidence for regulatory or legal reviews.
With quantum-enhanced verification protocols, the system can continuously validate whether financial data has been altered or corrupted. This real-time integrity monitoring enables organizations to detect anomalies instantly, maintain reliable financial reporting, and ensure compliance with accounting standards and regulatory requirements.

- **Implications for Accounting Functions**
  - **Financial Reporting**

Quantum-secured Accounting Information Systems (AIS) strengthen the trustworthiness of financial statements by ensuring that data is encrypted with advanced, future-proof security mechanisms. This minimizes the risk of unauthorized modifications and enhances confidence among investors, regulators, and stakeholders regarding the authenticity of financial reports. Quantum encryption and integrity-verification protocols detect even the smallest unauthorized change in accounting data. As a result, intentional manipulation, fraud, or accidental errors can be identified immediately, significantly reducing the possibility of financial misstatements and ensuring compliance with accounting standards.

  - **Auditing**

Quantum-secured audit logs record every transaction and system activity in real time with tamper-proof protection.

Auditors can continuously monitor financial processes instead of waiting for periodic audits, enabling early detection of irregularities, policy violations, or suspicious activities. Traditional auditing relies heavily on after-the-fact verification of records, which can be time-consuming and sometimes ineffective if evidence has been altered. With quantum-secured systems, verification occurs automatically and continuously, reducing the need for retrospective checks and improving audit efficiency and accuracy.

- **Corporate Governance**

Quantum-based security frameworks enhance internal control systems by ensuring only authorized users can access or modify financial information. This strengthens segregation of duties, reduces insider threats, and improves monitoring mechanisms across departments and organizational levels. When organizations adopt advanced security technologies like quantum-secured AIS, stakeholders perceive them as more transparent and accountable. Such systems also help firms meet stringent regulatory requirements related to data protection, auditability, and financial disclosure, thereby reinforcing corporate reputation and governance standards.

- **Challenges in Adoption**
  - **High cost of quantum infrastructure**

Implementing quantum-secured systems requires specialized hardware, advanced cryptographic tools, and high-performance computing infrastructure, which can be extremely expensive for most organizations. Small and medium enterprises may find the initial investment prohibitive, slowing widespread adoption despite long-term benefits.

  - **Limited quantum-skilled accounting professionals**

Quantum-secured AIS demands expertise that combines accounting knowledge with advanced cryptography and quantum computing concepts. Currently, there is a shortage of professionals trained in both domains, making implementation, maintenance, and auditing of such systems difficult.

  - **Integration with legacy ERP and AIS**

Many organizations still operate on traditional Enterprise Resource Planning (ERP) and Accounting Information Systems built without quantum-ready architecture. Integrating quantum security into these existing systems may require major system redesign, data migration, and compatibility adjustments, which can be technically complex and risky.

  - **Absence of accounting-specific quantum standards**

While general cybersecurity standards exist, there are no universally accepted accounting-specific frameworks tailored for quantum security. This lack of standardized guidelines creates uncertainty for organizations regarding best practices, compliance expectations, and implementation models.

- **Regulatory and Policy Implications**
  - **Need for quantum-security guidelines in accounting standards**

Standard-setting bodies may need to revise accounting and auditing standards to incorporate requirements related to quantum-safe encryption and data protection. Without formal guidelines, organizations may adopt inconsistent security practices, reducing comparability and reliability across financial reports.

  - **Role of regulators in promoting quantum-safe financial reporting**

Regulatory authorities play a crucial role in encouraging adoption through policy mandates, incentives, or compliance requirements. By establishing frameworks and monitoring adherence, regulators can ensure that financial information systems remain secure against emerging technological threats.

  - **Inclusion of quantum security in internal control frameworks**

Internal control models such as risk management and IT governance systems must evolve to include quantum-related threats and safeguards. Integrating quantum security into control frameworks strengthens organizational resilience and ensures that security considerations are embedded within operational and financial processes.

- **Scope of the research**
  - Future research can examine accountants' awareness, skills, perceptions, and willingness to adopt quantum-secured technologies. Such empirical studies would help identify training needs, adoption barriers, and behavioral factors influencing implementation success.
  - Scholars can conduct comparative research to evaluate differences in efficiency, security, reliability, and cost between traditional AIS and quantum-secured systems. This would provide evidence-based insights into whether the benefits justify the investment and technological transition.
  - Research can investigate how quantum security technologies influence audit accuracy, detection of anomalies, and reduction of fraudulent activities. Findings may demonstrate whether quantum-secured environments improve auditors' ability to provide assurance and strengthen financial integrity.

- Emerging economies present unique infrastructural, regulatory, and technological challenges that differ from developed markets. Studies focusing on countries like India can explore readiness levels, cost barriers, policy needs, and strategies for adopting quantum-secured accounting systems in resource-constrained environments.

2. CONCLUSION

Quantum-Secured Accounting Information Systems (AIS) signify a pivotal advancement in the domain of financial data management and security. By incorporating quantum-resistant encryption algorithms, tamper-proof audit mechanisms, and sophisticated quantum-based authentication protocols, these systems fundamentally transform the way financial information is stored, accessed, and verified. The integration of such quantum security technologies ensures that financial data remains confidential, immutable, and accessible only to authorized personnel, thereby significantly mitigating risks associated with cyber threats, data breaches, and fraudulent activities. As quantum computing continues to evolve, it poses an imminent threat to traditional cybersecurity frameworks, which rely heavily on classical cryptographic methods vulnerable to quantum attacks. Consequently, the transition to quantum-safe AIS is not merely advantageous but essential for maintaining the integrity and trustworthiness of financial reporting systems. Organizations that proactively adopt quantum-secured solutions will be better positioned to safeguard sensitive accounting data, enhance audit reliability, and uphold robust corporate governance standards. Furthermore, the implementation of Quantum-Secured AIS supports continuous auditing and real-time verification processes, enabling early detection of anomalies and unauthorized modifications. This enhances transparency and accountability, which are critical for meeting regulatory requirements and sustaining stakeholder confidence in an increasingly digital financial environment. Although challenges such as high implementation costs, integration complexities with legacy systems, and a shortage of quantum-skilled professionals remain, the long-term benefits of resilient, future-proof AIS frameworks underscore the strategic imperative for organizations to invest in quantum security technologies. In summary, Quantum-Secured Accounting Information Systems represent a necessary evolution in the accounting profession's response to emerging technological threats. By embracing these innovations, organizations can ensure the sustainability, reliability, and security of their financial information infrastructures in the post-quantum era

References

1. Demski, J. S., FitzGerald, S. A., Ijiri, Y., Ijiri, Y., & Lin, H. (2009). Quantum Information and Accounting Information: A Revolutionary Trend and the World of Topology. Journal of Accounting and Public Policy, 28(2), 133-147.

2. Kasheem, M., Shalghoum, N., & Abdullah, M. (2025). Impact of Quantum Computing on Accounting Information Systems: Challenges and Opportunities. SINOMIKA Journal: Publikasi Ilmiah Bidang Ekonomi dan Akuntansi, 4(1), 23-34.

3. Lazirko, M. (2023). Quantum computing standards & accounting information systems. arXiv preprint arXiv:2311.11925.

4. Mulla, Hajrabibi, (2025) Quantum Accounting: Challenges, Future Outlook, and Recommendations. Available at

5. SSRN: https://ssrn.com/abstract=5324442 or http://dx.doi.org/10.2139/ssrn.5324442

6. Shadan, Huma & Islam, Sardar. (2025). Quantum Computing and Cybersecurity in Accounting and Finance: Current and the Future Challenges and Opportunities for Securing Accounting and Finance Systems. 10.48550/arXiv.2506.12096.

7. Bell, E. (2020). Accounting Information Systems and Organizational Efficiency in Financial Reporting. gjstudies, 1(1), 8-8.

8. Ekici, H. (2025). The Impact Of Quantum Information Technologies On Accounting And Finance Applications. Journal Of Pure Social Sciences (Puresoc)-Pak Sosyal Bilimler Dergisi (Paksos), 6(10), 104-118.

9. Fellingham, J., & Schroeder, D. (2006). Quantum information and accounting. Journal of Engineering and Technology Management, 23(1-2), 33-53.

10. CFI Team(2020), Accounting Information System: Tools and Systems designed for the collection and display of accounting information, https://corporatefinanceinstitute.com/resources/accounting/accounting-information-system-ais/.