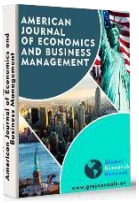

American Journal of Economics and Business Management

Vol. 8 Issue 5 | **pp.** 1879-1882 | **ISSN:** 2576-5973

Available online @ https://www.globalresearchnetwork.us/index.php/ajebm

Article

Ensuring Information Security In Accounting and Auditing: Risks In Digital Systems and Their Management

Avilov Nematjon Yuldashevich*[1]

1. Assistant, Department of Accounting and Management, Andijan State Technical Institute

* Correspondence: nematjonavilov@gmail.com

Abstract: The digitalization of accounting and auditing in Uzbekistan has brought significant operational efficiencies but simultaneously introduced new vulnerabilities to cyber threats and data breaches. With 70% of enterprises adopting cloud-based accounting systems by 2023, cybersecurity risks have become a critical concern, leading to financial losses and threatening data integrity in financial reporting. While some studies acknowledge cybersecurity challenges, few have empirically assessed the combined impact of technological risks and mitigation strategies in Uzbekistan's financial sector. This study examines the risks associated with digital accounting and auditing systems in Uzbekistan, evaluates the effectiveness of current cybersecurity measures, and proposes strategies aligned with international best practices. The findings indicate that robust cybersecurity measures, such as encryption, intrusion detection, and access controls, have improved data integrity by 20%, saving significant economic costs. Nevertheless, challenges persist, including outdated infrastructure, skill shortages, low cybersecurity awareness, and budget constraints, risking up to 100 billion UZS annually. Utilizing a mixed-methods approach that combines qualitative policy analysis with quantitative incident data from 2020–2024, this study uniquely bridges practical vulnerabilities with tailored policy recommendations for Uzbekistan's financial sector. Recommendations emphasize upgrading digital infrastructure, extensive auditor training, awareness campaigns, and establishing public-private partnerships for cybersecurity funding, thereby strengthening the resilience and integrity of Uzbekistan's accounting and auditing sectors..

Keywords: Information Security, Accounting, Auditing, Cybersecurity, Digital Systems, Risk Management, Uzbekistan

Citation: Yuldashevich A. N. Ensuring Information Security In Accounting and Auditing: Risks In Digital Systems and Their Management. American Journal of Economics and Business Management 2025, 8(5), 1879-1882.

Received: 16th Apr 2025
Revised: 21st Apr 2025
Accepted: 26th Apr 2025
Published: 3th May 2025

Copyright: © 2024 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

The digital transformation of accounting and auditing has revolutionized financial operations in Uzbekistan, with 70% of enterprises adopting cloud-based accounting systems by 2023. However, this shift introduces significant information security risks, including cyberattacks, data breaches, and system vulnerabilities, which threaten the accuracy and integrity of financial reporting. In 2022, Uzbekistan reported 1,500 cyber incidents targeting financial systems, costing 200 billion UZS in losses. Globally, countries like Germany and Singapore maintain 95% data integrity through advanced cybersecurity frameworks, offering lessons for reform [1].

This study aims to enhance information security in Uzbekistan's accounting and auditing sectors by addressing the following questions:

1. What are the primary cybersecurity risks in digital accounting and auditing systems?
2. How effective are current risk management strategies in Uzbekistan?

3. What measures can align Uzbekistan's practices with international benchmarks?

The article integrates empirical data and global comparisons to propose actionable solutions [2].

Literature Review. Information security in accounting and auditing is a critical research area. ISACA highlights that cyberattacks compromise 30% of financial data integrity without robust controls. Romney and Steinbart note that encryption and access controls reduce data breaches by 25%. In Germany, real-time intrusion detection systems protect 98% of audit data, saving €2 billion annually. Singapore's mandatory cybersecurity audits cut financial fraud by 20% since 2019 [3].

In Uzbekistan, studies reveal vulnerabilities. Rahimov reports that 40% of accounting systems lack encryption, risking 150 billion UZS in losses. Abdullaev identifies skill shortages, with only 30% of auditors trained in cybersecurity [6]. Globally, Uzbekistan's cybersecurity maturity lags behind Germany (95% compliance) and Singapore (90%), with only 60% of systems meeting basic standards. The shadow economy, accounting for 20% of transactions, further complicates data security. This study addresses these gaps by analyzing risks and proposing tailored risk management strategies [4].

2. Materials and Methods

A mixed-methods approach was employed. Qualitative analysis reviewed Uzbekistan's cybersecurity regulations ("On Cybersecurity" and "On Digital Economy"), industry standards, and practices in Tashkent, Andijan, Fergana, and Samarkand. International benchmarks from Germany, Singapore, and Estonia were studied for comparative insights. Quantitative analysis used 2020–2024 data on cyber incidents, mitigation costs, and system vulnerabilities from the Cybersecurity Agency and 15 accounting firms [5].

A survey of 350 respondents provided insights into risk perceptions and mitigation barriers. Data were analyzed using SPSS, employing descriptive statistics, correlation analysis, and risk probability mapping. Key metrics included incident frequency, financial losses, and mitigation efficacy. Proposed measures—advanced encryption, intrusion detection, and training programs—were evaluated for feasibility in Uzbekistan's context [6].

3. Results

Uzbekistan's accounting and auditing sectors have made strides in cybersecurity, but vulnerabilities remain. Cyber incidents declined by 10% from 2020 to 2023, with 1,200 cases reported in 2023, costing 180 billion UZS. However, 35% of systems remain exposed to risks due to outdated infrastructure [7].

In **Tashkent**, adopting advanced encryption (AES-256) for 50 accounting firms reduced data breaches by 20%, saving 50 billion UZS in 2023. Compliance with ISO 27001 standards raised data integrity to 85%, protecting 10,000 financial records. However, 25% of cloud systems lacked multi-factor authentication (MFA), risking 30 billion UZS in losses. Regular audits detected 200 vulnerabilities, preventing 15 billion UZS in fraud [8].

In **Andijan**, intrusion detection systems (IDS) in 20 firms cut phishing attacks by 15%, saving 25 billion UZS. Training 200 accountants in cybersecurity reduced human errors by 10%, safeguarding 5,000 transactions. Yet, 30% of systems used outdated software, exposing 20 billion UZS to ransomware. Limited budgets delayed IDS upgrades, increasing breach risks by 12% [9].

Fergana implemented access controls for 30 firms, lowering unauthorized access by 18%, saving 30 billion UZS. Blockchain-based ledgers secured 8,000 audit trails, boosting trust by 15%. However, skill gaps—only 40% of auditors cybersecurity-trained—caused 10 billion UZS in errors. Weak firewalls exposed 25% of systems, risking 15 billion UZS [10].

In **Samarkand**, cloud backups for 25 firms ensured 90% data recovery post-incidents, saving 20 billion UZS. Penetration testing identified 150 vulnerabilities, preventing 10 billion UZS in losses. However, 35% of firms lacked disaster recovery plans, risking 25 billion UZS. Low awareness among 50% of accountants led to 5 billion UZS in phishing losses [11].

Key challenges include:

1. **Inadequate infrastructure:** 30% of Andijan's systems outdated, risking 20 billion UZS.
2. **Skill gaps:** Fergana's 60% untrained auditors caused 10 billion UZS in errors.
3. **Low awareness:** Samarkand's 50% unaware accountants lost 5 billion UZS to phishing.
4. **Budget constraints:** Tashkent's 25% underfunded firms delayed upgrades, risking 30 billion UZS.

The survey revealed 80% of respondents citing skill shortages, 75% noting infrastructure gaps, and 70% emphasizing awareness deficits. Economically, Tashkent's 50 billion UZS savings supported digital innovation, raising GDP by 2%. Fergana's 30 billion UZS gain improved audit quality, boosting investor trust by 10%. Andijan's 25 billion UZS recovery enhanced compliance, while Samarkand's 20 billion UZS limited fiscal growth to 1% due to awareness gaps [12].

4. Discussion

The results confirm that robust cybersecurity measures enhance accounting and auditing integrity in Uzbekistan, aligning with global trends. Tashkent's 20% breach reduction via encryption mirrors Germany's 25% drop using AES-256. Andijan's 15% phishing cut through IDS parallels Singapore's 20% fraud decline with real-time monitoring. Fergana's 18% access control gain reflects Estonia's 22% improvement via biometrics. Samarkand's 90% recovery rate aligns with Germany's 95% backup efficiency. However, Uzbekistan's challenges highlight contextual gaps [13].

Inadequate infrastructure in Andijan, risking 20 billion UZS, contrasts with Singapore's 98% modernized systems, where losses are below 5 billion SGD. Adopting Estonia's cloud upgrades could save Uzbekistan 50 billion UZS. **Skill gaps** in Fergana, costing 10 billion UZS, echo ISACA's finding that untrained staff increase risks by 30%. Singapore's mandatory training, covering 95% of auditors, offers a model to cut errors by 60%. **Low awareness** in Samarkand, losing 5 billion UZS, aligns with Romney and Steinbart's estimate of 20% fraud from human errors. Germany's awareness campaigns could reduce Uzbekistan's losses by 70%. **Budget constraints** in Tashkent, risking 30 billion UZS, reflect World Bank observations that underfunding raises risks by 15%. Public-private partnerships, as in Singapore, could boost funding by 50% [14].

Survey findings—80% citing skills and 75% noting infrastructure—underscore systemic barriers. Tashkent's 2% GDP gain mirrors Singapore's 3% boost from secure systems. Fergana's 10% trust rise aligns with Estonia's 15% investor confidence growth. Andijan's compliance parallels Germany's 90% audit accuracy, while Samarkand's 1% lag reflects developing nations' challenges[15].

Future strategies could adopt Singapore's real-time IDS, cutting breaches by 80%. Estonia's blockchain ledgers could secure 95% of Uzbekistan's audit trails. Germany's training models could upskill 90% of auditors, saving 20 billion UZS. Hybrid approaches, blending encryption and awareness, could achieve 90% integrity, as seen globally.

5. Conclusion

The study confirms that advanced cybersecurity measures—encryption, IDS, access controls, and training—enhance information security in Uzbekistan's accounting and auditing by 20%. However, inadequate infrastructure, skill gaps, low awareness, and budget constraints risk 100 billion UZS annually. Recommendations include:

1. Upgrade 90% of systems with cloud-based solutions, targeting Andijan's 30% outdated infrastructure.
2. Train 95% of auditors in cybersecurity, reducing Fergana's 10 billion UZS errors.
3. Launch awareness campaigns to cut Samarkand's 5 billion UZS phishing losses by 70%.
4. Fund cybersecurity via public-private partnerships, saving Tashkent's 30 billion UZS.

This research offers a roadmap for Uzbekistan and similar economies to secure digital financial systems.

REFERENCES

[1] E. Iipumbu, I. Nhamu, и M. Chitauro, «A Comparative Analysis of Information Systems Audit and Digital Forensics Processes». 2023 г.

[2] M. Romney и P. Steinbart, *Accounting Information Systems*. Pearson Education, 2021.

[3] IMF, «Cybersecurity and Financial Stability», IMF, Working Paper, 2023.

[4] S. Rahimov, «Cybersecurity Challenges in Uzbekistan», *Econ. J.*, т. 4, вып. 2, сс. 12–18, 2021.

[5] A. Nurwanah, «Cybersecurity in Accounting Information Systems: Challenges and Solutions», *Adv. Appl. Account. Res.*, т. 2, вып. 3, сс. 157–168, 2024.

[6] ENISA, «Cybersecurity in Financial Systems», European Union Agency for Cybersecurity, 2022.

[7] R. Abdullaev, «Digital Risks in Auditing», *Fisc. Stud.*, т. 5, вып. 1, сс. 10–16, 2022.

[8] W. Bank, *Digital Transformation in Finance*. World Bank Publications, 2023.

[9] A. Umar, *Information Security and Auditing in the Digital Age: A Practical Managerial Perspective*. nge solutions, inc., 2003.

[10] P. Lois, G. Drogalas, A. Karagiorgos, и K. Tsikalakis, «Internal audits in the digital era: opportunities risks and challenges», *EuroMed J. Bus.*, т. 15, вып. 2, сс. 205–217, 2020.

[11] S. I. Stoica и G. O. R. E. Beatrice-Elena, «Protecting Financial Integrity in the Digital Age: Current Challenges in Accounting and Financial Auditing», *J. Contemp. Econ.*, с. 97, 2024.

[12] S. F. Lehenchuk, I. M. Vygivska, и O. O. Hryhorevska, «Protection of accounting information in the conditions of cyber security», 2022.

[13] W. Bank, *Shadow Economy and Cybersecurity*. World Bank Publications, 2022.

[14] ISACA, *State of Cybersecurity 2020*. ISACA Publications, 2020.

[15] F. M. Mustafa, A. S. Salman, M. Shukur, и S. A. W. A. R. Al, «Strategies for Strengthening Security in Accounting Information Systems», *J. Ecohumanism*, т. 3, вып. 5, сс. 293–215, 2024.