Requirements and challenges facing electronic accounting information systems in enhancing financial information security

DJABALLAH Adel Ryad*[1], BENHAMMOUDA Mahboub[2]

[1] Researcher lecturer B, University of Algiers 3, Laboratory of Traditional Industiers, adel.ryad@live.fr

[2] Professor, University of Algiers 3, Laboratory of Traditional Industiers, prbmahboub@gmail.com

Received: 24/05/2026 *Accepted: 18/06/2026*

Abstract:
This paper analyzes the importance of Electronic Accounting Information Systems (EAIS) in improving the security of financial information in modern organization, by addressing the conditions that must be in place to ensure the successful implementation of EAIS such as the technological infrastructure, internal control systems and the knowledge of the employees. Nevertheless, the most important challenges are known to be cybersecurity threats, system integration issues, and a lack of awareness by the users. The paper provides an understanding of the importance of EAIS in promoting integrity and reliability of financial information, which in turn allows making informed managerial decisions and transparency in the organization as a result of critically analyzing seventeen peer-reviewed, scholarly sources.

Keywords: Electronic Accounting Information Systems, Financial Information Security, Cybersecurity, Internal Controls, Cloud Computing, Blockchain Technology, Competency of the Staff.

Jel Classification Codes: M40, M41, M42, M15, D8, G20, G23, G33, G32,J24.

* **DJABALLAH Adel Ryad**

1. INTRODUCTION

Digitalization of the business processes has totally changed the way financial data is managed and kept secure in organizations. Electronic Accounting Information Systems (EAIS) started as conveniently-simplified automation solutions, however, currently are a full-fledged system that includes such modern technologies as artificial intelligence, blockchain, cloud computing, and big data analytics (Al Tarawneh et al., 2023). Though this transformation has given unprecedented opportunities in efficiency and transparency the transformation has given rise to very complex security concerns that organizations must consider to maintain the integrity and reliability of financial data.

Fiscal data security refers to the protection of accounting data against fraudulent access, tampering, and theft, its accuracy, integrity, and confidentiality (Nurwanah, 2024). In the modern context of sophisticated cybercrime, regulatory pressure, and escalating demands of stakeholders to know more about their financial information, the role of EAIS in improving the financial information security has taken the first place. Businesses are now being pressurized to implement robust systems which not only automate accounting practices but offer an overview of a security system that is inclusive to offer protection on sensitive financial information.

The significance of the proposed study is in the fact that it examines in depth the requirements and the problems of EAIS implementation within the frames of financial information security. Though the current literature is applicable to the subject under study, as it concentrates on specific elements of accounting information systems, the area has a considerable gap in the research by incorporating technology, organizational, and human factors, which can impact the safety of financial data (Monteiro et al., 2022). The paper addresses this gap by providing a combination of frameworks addressing different aspects of EAIS security according to the most current academic sources.

There are three major objectives of this research. First, to identify and analyze the most significant needs that were necessary to realize EAIS successfully, such as technological infrastructure, internal control tools, and employee competence. Second, to examine the biggest barriers to achieving the objective of financial information security such as cybersecurity threats, issues with system integration, and user lack of awareness. Third, to present evidence-based proposals to organizations that are interested in improving organizational financial information security through the application of strategic EAISs. Through the discussion of such goals, this study adds to the academic and practical topics of accounting information system.

2. Literature Review and Theoretical Framework

2.1 Electronic Accounting Information System History:

Among the most significant change that occurred to the technology in business is the overhaul of accounting that was initially in form of manual ledgers to highly computerized operations. Electronic Accounting Information Systems are the integration of various technological factors aimed at supporting the process of

automation of the financial sphere, real-time analytics, and decision-making (Monteiro et al., 2022). The present day EAIS has numerous layers of functionality that include transaction processing, financial reporting, management accounting and audit support which are well supported by effective security. The recent research confirms that the quality of EAIS could significantly influence the generation of quality information on accounting that would have a positive effect on the success of organizational decision-making and performance that are not financial (Ahmed, 2019). The inclusion of the latest technologies, such as blockchain, artificial intelligence, and cloud computing, has only made the EAIS even more powerful. This has seen companies become capable of enhancing the security, efficiency, and transparency of their financial operations.

2.2 Theoretical Basis:

To identify the implementation of EAIS and security, this work will be premised on three complementary hypotheses. To start with, one can analyse the impact of organisational characteristics, organisational environment, and technical capabilities on EAIS uptake and performance with the help of the Technology-Organization-Environment (TOE) framework (Nurwanah, 2024). This paradigm acknowledges that the organisational readiness and technology recommendations should be the same to achieve success in EAIS deployment.

Second, the nature of dependency between the technical systems and the human actors is also highlighted by the Socio-Technical Systems (STS) theory. According to it, the element of EAIS security depends not only on the technological defense but also on the corporate culture, how the users behave and the assistance that the management offers (Nurwanah, 2024). This argument may be particularly applicable to take into consideration that the human factor remains a major vulnerability of financial information security.

Third, one of the models that enables the evaluation of the effectiveness of EAIS in numerous dimensions is the DeLone and McLean Model of Information Systems Success, which can be applied to assess its quality in the system, quality of information, quality of service, user satisfaction, and net benefits (Monteiro et al., 2022). The model helps the companies to determine the capability of their EAIS implementations to achieve the desired security and performance outcomes.

3. Key Requirements for Effective EAIS Implementation

3.1 Technological Infrastructure Requirement:

The basis of secure EAIS lies in the strong technological platform that can deal with sophisticated financial transactions and achieve a high degree of security, reliability, and performance. The organizations are forced to invest in hardware, software, network infrastructure, and data storage technologies that satisfy the latest security requirements and can support the growth.

- **Advanced Security Technologies:**

The modern EAIS demands several levels of security to prevent any threats to financial information. Encryption solutions provide secure information flow of financial data, and organizations are starting to use even higher encryption standards, such as AES-256, to protect data (Nurwanah, 2024). Multi-factor authentication (MFA) is now a mandatory feature, providing an extra verification procedure beyond standard passwords to prevent unauthorized access (Nurwanah, 2024).

The technologies of artificial intelligence and machine learning are being used more and more to detect and react to threats in real time. They allow analyzing large amounts of transaction data to find any suspicious patterns that may reflect the possibility of fraud or a security breach and mitigate the threat faster and more efficiently (Barreto et al., 2025). Nonetheless, companies should also understand that the AI systems do not come without their own risks, such as the risk of data bias and vulnerability to adversarial attacks (Nurwanah, 2024).

- **Cloud Computing Infrastructure:**

Cloud computing has become the most revolutionary technology in EAIS, providing cost savings, scalability, flexibility, and real-time availability (Monteiro et al., 2022). Cloud-based accounting systems allow organizations to have access to financial information from any place with internet access, allowing remote working and collaboration and lowering the costs of infrastructure (Hamdan et al., 2019).

Nevertheless, there are certain security concerns that are brought with cloud adoption. It is the responsibility of an organization to see that cloud service providers have in place proper security mechanisms, which could include data encryption, access rights, and recovery mechanisms in the case of a disaster. Data loss or leakage, open application programming interface, poor infrastructure design, and unknown risk profile are security threats unique to the cloud environment. Research indicates that cloud accounting integration and security/privacy concerns are the key factors that contribute to cloud accounting adoption, which implies that cloud accounting implicates these concerns should one implement cloud computing accounting (Fitriati and Susanto, 2017). In order to address the cloud risks, companies will conduct an appropriate evaluation of the vendors, develop clear service level agreements, and introduce other security provisions.

- **Integration of Blockchain Technology:**

The blockchain technology is an innovation in the accounting information systems, and the degree of transparency, security, and data integrity were never witnessed before. Blockchain decentralization and immutability offer an assurance that a digital record of the financial transactions could not be altered or deleted once it was entered into the blockchain, eliminating the potential of fraud to a large degree (Secinaro et al., 2021).

The findings of recent studies indicate that the efficiency of the information sharing, accuracy of data sharing, and the cost of sharing financial information in the accounting system improve by 25.7, 19.8, and 13.6, respectively, when blockchain is utilized instead of traditional methods (Fitriati and Susanto, 2017). Blockchain, in

particular, distributed ledger technology, eliminates the existence of intermediaries in the context of different financial transactions to reduce the cost of transactions and improve the efficiency of operations (Cong & He, 2018).

Self-executing contracts, commonly known as smart contracts, allow financial operations to be automated and follow the established rules. This automation minimizes the involvement of human beings, therefore, limiting chances of manipulation or error. Nonetheless, blockchain adoption is associated with such weaknesses as scalability, excessive energy use, lack of compatibility with current systems, and special technical skills (Fitriati & Susanto, 2017).

3.2 Internal Control Mechanisms:

Internal control systems are another vital aspect of EAIS security that contains the means of accuracy, fraud prevention, compliance, and asset security of the organization. According to the Committee of Sponsoring Organizations (COSO) framework, there are five interrelated components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring (Adil et al., 2025).

- **Control Environment and Governance:**

The environment of control provides the basis of all the internal control activities that are based on the organizational culture, ethics, and philosophy of risk and control by the management of the organization. It was shown that a good organizational culture, focusing on cybersecurity, has a tremendous impact on adherence to security policies and decreases the risk of being exposed to cyber threats (Nurwanah, 2024).

To realize good internal control implementation, top management support is needed. Research indicates that companies where the management is highly committed to the internal controls have high-quality systems and improved financial reporting results (Nurul, 2025). The management should also invest sufficient resources, set proper policies, and show uniform interest in security principles.

- **Segregation of Duties and Access Controls:**

Separation of functions ensures that no single party has the power to do whatever they like in the financial operations, hence decreasing fraud or error chances. This principle can be applied in an electronic setting, where access to the system is limited by role-based access controls, which govern user access based on job roles and needs (Adil et al., 2025). Digitization of accounting information systems will be able to support more advanced access control (i.e., more dynamically authorized systems), in which permissions vary by context, time, and risk-level (Daway et al., 2025). The least privilege principle needs to be implemented in the organizations where users are granted as limited access as they need to fulfill their work, and access rights are to be periodically checked to ensure that they are sufficient.

- **Risk Monitoring and Assessment:**

The threats to organizational goals are produced and analyzed by the current risk evaluation process and therefore their mitigation plans can be carried out. Regarding EAIS, the risk assessment should be focused on both conventional financial

risks and the new cybersecurity threats (Fitriati & Susanto, 2017). The current-day EAIS also includes automated monitoring features that constantly scan transactions and system activity to identify anomalies indicative of a security breach or control failure (Daway et al., 2025). These systems are machine learning-based algorithms that create baseline patterns of behavior and then alert on any deviations that need to be investigated. Monitoring of the security in real time allows responding to the incidents faster, which reduces the possible harm.

3.3 Staff competency and training requirements:

The importance of human factors in EAIS security is evident, and studies have yet to prove that the lack of user awareness and insufficient training is a major weakness (Nurwanah, 2024). Companies should invest in the training of employees to have competencies that facilitate the use of accounting information systems in an effective and secure way.

- **Digital Skill and Technical Competencies:**

The digitalization of accounting has radically changed the nature of required competencies; 67% of the existing knowledge and skills required of accountants are connected to digital competence (Zhu, 2022). The contemporary accounting professional should have such technical skills as data analytics, data expertise in cloud computing, knowledge of cybersecurity principles, and the capacity to operate with the new technological transformations like artificial intelligence and blockchain (Barreto et al., 2025). Studies determine that there are some essential digital competencies of accounting professionals. These are the skills to become proficient when using accounting software and tools, the skills to analyze data sets, proficiency in the principles and practices of information security, the awareness of the new technologies and their usage, and the skills to adapt to the quickly changing technological conditions (Barreto et al., 2025).

- **Cybersecurity Awareness and Training:**

The concept of cybersecurity awareness is an essential skill because human error is a major contributor to security attacks. Organizations need to introduce intensive training initiatives to cover the topics of threat identification, good passwording, phishing and social engineering education, incident reporting protocols, and data management and privacy specifications (Cherian, 2025). There is evidence that mandatory cybersecurity training, frequent changes in the upsurge of new threats, and fostering the organizational culture that is security-awareness play an important role in enhancing the security posture (Nurwanah, 2024). The training needs to be a continuous process, not an event, and it should keep pace with emerging new threats and technologies. Regular testing (simulated phishing exercises, etc.) should also be carried out in organizations to determine the level of training and determine which areas need more attention.

- **Continuous Professional Development:**

The high rate of technology change also requires lifelong learning and constant acquisition of new skills. This need is becoming more accepted by professional

accounting organizations, as professional accounting bodies, including the South African Institute of Chartered Accountants, highlight that accountants need to be continually changing in order to be relevant and competitive (Chandler, 2024). Developed professional development programs such as formal training programs on new technologies and security practices, industry conferences and workshops, access to online learning programs and resources, mentoring programs matching experienced and novice employees, and the possibility to test new technologies in controlled settings should be developed by organizations (Chandler, 2024).

4. Significant Problems in the Attainment of Financial Information Security

4.1 Cybersecurity Threats and Vulnerabilities:

The cybersecurity environment has become extremely dynamic and dangerous, and attacks on accounting firms have increased by 300 percent since 2020. Companies have to deal with several types of cyber attacks that may lead to information security issues with their finances. Malicious code attack vectors are sophisticated, complex, and can be exploited to carry out intrusions.

- **Advanced Attack Vectors**

Attacks involving phishing have not only progressed as straightforward email scams but also involved some more advanced methods, such as deepfake technology, which involves using artificial intelligence to generate credible impressions of business executives or close contacts. Studies show that the number of fraudulent attempts with the deepfakes grew by 3,000, which is a drastic turn towards the level of threats (Hyde, 2023).

Ransomware is also a major issue, with 65 percent of financial services organizations experiencing ransomware in 2024, and the average cost of recovery going up to 2.73 million dollars (Tamzid, 2025). Contemporary ransomware attacks have a tendency to utilize double extortion schemes, where data is encrypted, but it is also exfiltrated, and threats to expose the information publicly are made without the need to make further payments.

Both intentional and unintentional insider threats are some of the main causes of accounting data breaches. Insider threats have long been highlighted by the American Institute of Certified Public Accountants as a concern that has been intensifying as companies decide to work remotely and use common clouds (Tamzid, 2025). Simple errors, unsuccessful data management inside the company, and excessive permissions are all sources of major security incidents.

- **Advanced Persistent Threats:**

Advanced Persistent Threats (APTs) are complex and long-term cyberattacks, usually performed by nation-state agencies or deep-pocket criminal groups. APTs use covert methods to continue having a long presence in the target networks, stealing confidential information or preparing future attacks (Cherian, 2025). Such threats demand sophisticated detection techniques such as behavioral analysis, integration of threat intelligence, and continuous observation.

4.2 System Integration Challenges:

The implementation of EAIS and integration with the existing organization systems is a significant technical and organizational problem. Organizations generally have several systems that meet various functional areas, and the need to ensure smooth integration does not come easily, yet security is a concern.

- **Legacy System Compatibility:**

The systems in place in most organizations are considered old and did not have the capability of supporting the current security and integration needs. Combining them with contemporary EAIS can be a security threat, particularly in case legacy systems lack the appropriate access controls and even encryption capabilities (Han et al., 2023). Enterprises have to weigh the system integration requirements with the security requirements, and they usually demand huge sums of money in the middleware, API, or even the replacement of the entire system. This is a particularly acute problem for small and medium-sized enterprises that have limited funds for infrastructure modernization.

- **Interoperability and Data Consistency:**

It is important to ensure that the data in integrated systems is consistent to ensure the integrity of financial information. In the case of exchanging data among more than two systems, organizations need to introduce effective data validation, transformation, and reconciliation procedures to avoid mistakes or discrepancies (Cong & He, 2018). The use of blockchain with the current accounting systems is typical of interoperability issues. Although blockchain has such a considerable advantage of security, the application of decentralized blockchain systems with the current centralized database involves the need to resolve the so-called mapping problem between on-chain and off-chain data (Cong & He, 2018). The companies should come up with validation systems to guarantee the correlation of blockchain data with the real operational records.

4.3 Regulation Compliance and Legal Concerns:

The organizations that use EAIS have to deal with multifaceted and dynamic regulatory environments that deal with data security, financial reporting, and cybersecurity and privacy. The rule of compliance also differs across jurisdictions, which introduces another multifaceted problem of multinational organizations.

- **Data Protection and Privacy Regulations:**

Laws like the General Data Protection Regulation (GDPR) in Europe and other laws in other parts of the world place severe restrictions on the manner in which an organization gathers, processes, stores, and safeguards personal information (Monteiro et al., 2022). The implementation of EAIS should have the option of features that help in compliance with such regulations, such as data subject rights management, breach notifications, and privacy by design. The use of cloud-based EAIS has specific issues related to data sovereignty and inter-country data transfer because regulations can limit the storage and access to financial data location and form. When identifying cloud

service providers and configuring systems, these are the requirements that organizations need to take into consideration carefully.

4.4 Financial Reporting and Audit Requirements:

EAIS should be capable of complying with the regulations of financial reporting, like International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Principles (GAAP). The systems should have sufficient audit trails, data integrity, and external auditors should be able to check financial information. New technologies, such as blockchain, bring new audit challenges because it is possible that the traditional audit processes would not be sufficient to cover the decentralized system or smart contracts. Even professional accounting organisations have yet to design information on the audit of blockchain-based financial records, and this leaves organisations implementing such technology in a state of uncertainty.

- **Resource Limitations and Implementation Costs:**

Both financial and human resource constraints have a major influence on the capacity of organizations to adopt full EAIS security protocol, especially for small and medium enterprises.

- **Financial Investment Requirements:**

To establish an efficient EAIS with the relevant level of security, it will take significant financial investments in the hardware infrastructure, software licensing, cloud services, security tools and monitoring systems, staff training and development, and continuous maintenance and updates (Nurwanah, 2024). SMEs usually do not have the resources to effectively do full security implementations, and as a result, they have been faced with hard decisions between investing in security and other areas of their business. The inequity in resources offers a two-level security situation in which massive organizations are in a position to offer advanced security systems, whilst smaller parties are at risk.

4.5 The Lack of Qualified Personnel:

There is a serious shortage of skilled information technology and cybersecurity experts, exacerbating resource issues. Organizations are vying for the scarce resources of talent in terms of people who have the required technical expertise, cybersecurity, accounting, and knowledge of regulatory mandates (Zhu, 2022). This skills mismatch is especially sharp in the undeveloped world, as educational systems might not have been kept abreast of industry requirements of digital skills (Chandler, 2024). Organizations are forced to pay a lot of money to develop and train their current employees, or have to go through extended periods of office vacancy due to critical vacancies in the security sector.

- **Organization Culture and Change Management:**

To be successfully implemented, the EAIS will involve a major change in the organization in terms of work processes, roles, and responsibilities. The unwillingness to change and poor management of change are significant obstacles to successful implementation.

- **User Resistance and Adoption Challenges:**

Employees may be opposed to new systems due to fear of job loss, aversion to technology, and the fact that a new system can impose an extra workload during the transition period, or doubt about the advantages of the new system (Cong & He, 2018). This opposition may compromise security by promoting workarounds, failure to adhere to procedures, or even low system usage. Resistance in organizations needs to be overcome by effective communication on the reasons why systems should be implemented and the benefits, inclusion of the final users in the system selection and design stages, full training and support, and overt management commitment and leadership (Nurwanah, 2024).

- **Security Culture Development:**

The development of an organizational culture that places emphasis on information security is a long process that requires the dedication of the leadership. The studies have shown that organizations that have high security cultures have fewer security incidents and improved adherence to security policies (Nurwanah, 2024).

The security culture can be developed by including security in organizational values and mission, frequent security awareness messages, rewarding and recognizing security-aware behavior, openness to discuss security incidents, without over-blame, and maintaining the imposition of policies on security across all levels of the organization. Leaders should be able to set the right security behaviors and show that security is not an exercise of compliance but a value that is deeply ingrained in the organization.

5. CONCLUSION

Electronic Accounting Information Systems are imperative infrastructures of the existing organizations that strive to possess a competitive advantage and financial information integrity and safety. This overhaul analysis has revealed essential needs such as well-developed technological support, strong internal controls, competency of staff, and high quality of information. At the same time, the paper has demonstrated the major challenges including cybersecurity risks, complexity of integrating the system, data integrity, cloud security, regulatory compliance requirement, and user resistance.

The studies prove that effective implementation of EAIS must be based on comprehensive methods of approach that consider technical, organizational, and human aspects. Organizations cannot just use technological solutions only but they have to develop security aware cultures, proper governance frameworks, relevant training, and continuous improvement. The interdependence of the requirements and challenges requires combined approach instead of focusing on the separate issues and providing solutions to them individually.

The need of effective and safe EAIS will be even more important as the digital transformation keeps transforming the business processes. Companies that are truly dynamic in responding to the needs of their customers, as well as the predicaments

they may be facing by undertaking wholesome, well-thought processes in implementing the systems will be in a better position to safeguard their financial information resources as well as enjoy the benefits of the electronic accounting systems. Further studies must be carried on the issue of new technologies and threat environment in order to offer new advice to practitioners in this complex and dynamic environment.

The research of this paper can have a beneficial practical effect on managers, IT specialists, and accounting professionals involved in the implementation or maintenance of EAIS. Knowing what is needed to succeed and what the pitfalls would be, these stakeholders can make more knowledgeable decisions, distribute resources better, and build stronger strategies on how to improve the security of financial information with the help of electronic accounting information systems.

- Discussion:

As demonstrated in the analysis of this research, the implementation of EAIS financial information security needs balancing of various conflicting demands, and handling of challenges on technological, organizational, and human levels. Organizations have to deal with the conflict between innovation and security, functionality and control, investment and return.

The literature has many major themes. To start with, it is evident that technological solutions cannot be used in the context of realizing financial information security on their own. Although technologies such as blockchain, artificial intelligence, and cloud computing offer immense security advantages, their usefulness is heavily reliant on organizational variables, including management support, internal controls, and user behavior (Nurwanah, 2024).

Second, the study finds that there exists a notable gap between the existing technologies and the organizational ability of exercising them appropriately. The lack of capacity is actually reflected through various aspects, such as the lack of technical skills, financial resources, user awareness and training, and underdeveloped security cultures (Barreto et al., 2025). To resolve such capacity constraints, there is a need to invest in human capital development and organizational change management in the long term.

Third, the dynamic nature of the threat environment involves the need to keep on learning and adapting. In one time, organizations should not propel EAIS security activities, but they should establish some measures that will oversee, assess, and optimize the existing processes to fulfill the arising threats and technologies (Nurwanah, 2024). This pressure to remain abreast with change creates more pressure on already strained organizational resources.

The organizational contexts are also interesting differences having been discovered through the research. Full security measures that entail the deployment of diverse advanced technologies and security officers can be afforded by the big organizations with a massive budget. In their turn, the small and medium-sized enterprises are faced with the task of adequately securing the adequate levels as they lack the resources (Nurwanah, 2024). This gap would mean that there would be

gradual security measures which should be proportionate to the size and the resources of the organization. The regulatory environment has a significant influence on the EAIS implementation strategies, and companies operating in an environment or jurisdiction that is highly regulated have additional compliance costs and requirements. However, the advantages of the improved security are also the outcome of regulations, which introduce the minimum standards and offer a possibility to hold the security failures responsible.

- Best Practices and Recommendations:

- **Adopting a Comprehensive Security Framework:**

Companies ought to embrace holistic security models that can handle both the technological, organizational, and human aspects. COBIT (Control Objectives for Information and Related Technologies) and COSO (Committee of Sponsoring Organizations) are frameworks that should be combined to offer systematic ways of handling information technology and internal controls (Daway et al., 2025).

The principles of holistic approach are founded on the premise that technology does not assure security; organizational processes, policies and human behaviors must be aligned with the capabilities of technology. The organizations should conduct periodic security tests which unveil the weaknesses of all the dimensions, implement the layered security measures which would assist in addressing the multitude of the threat vectors, have a well defined governance structure with the roles and responsibilities defined, and undergo an ongoing monitoring and improvement process.

- **Priority to User Education and Awareness:**

Since human factors are still a major security weakness, organizations should focus on extensive and continuous educational initiatives. It is necessary to customize these programs according to various organizational functions, counteract the emerging threats in real-time, apply interesting teaching techniques such as simulations and exercises, and evaluate the results by means of testing and evaluation (Cherian, 2025). Organizations also ought to promote the culture of speaking up, where employees should be able to report in case there is any suspicious activity or even a possible security incident without fear of any consequences. Security incidents could be highly mitigated by early notification and reporting.

- **Adopting Risk-Based Approaches:**

Risk-based strategies should be adopted by organizations where the security resources are assigned on a proportional basis to the number of threats and impacts identified. This includes carrying out periodic risk assessment that pinpoints and prioritizes risks, controls that tackle the risk areas with the highest risk should be implemented first, monitoring of risk landscapes to identify new threats, and making adjustments to security strategies to align with new threats (Nurwanah, 2024). Risk-based methods allow organizations to develop the maximum security benefit with limited resources because investments are made in areas that are the most vulnerable or the most likely to be affected.

- **Leveraging Strategic Partnerships:**

Strategic partnerships should be considered by the organizations in order to cope with the limitations of resources and expertise. This involves the services of managed security service providers to monitor and respond to an incident, engaging cloud service providers with advanced security services, joining information sharing and analysis centers to exchange information on threats, and cooperating with educational institutions to develop the workforce. Strategic alliances help organizations to gain access to capabilities and knowledge previously unattainable by the company through internal means and potentially at a high cost.

- **Incident Response and Recovery Planning:**

In spite of the best preventive measures, security incidents will be experienced. Companies should develop comprehensive incident response strategies that encompass detection and identification of incidents, containment and eradication measures, recovery and restoration, post-incident analysis and learning, and stakeholder communication (Nurwanah, 2024). Tabletop exercises or simulation of incident response plans on a regular basis are used to ensure that organizations are ready and need improvements.

- Limitations and Future Research Directions:

This study has a number of limitations that ought to be noted. To begin with, the research only uses published academic content, which might not adequately reflect the emerging practice and new advances yet to be contained in peer-reviewed journals. Second, the limited generalizability of studies in other contexts may be a problem due to the geographic and organizational diversity of studies included. Third, the high rate of technological change means that some of the results will be exposed to obsolescence as new technologies and threats occur.

There are a number of crucial areas that need to be covered in future research. To start with, findings of empirical studies on the effectiveness of various EAIS security methods in different organizational settings would be of great practical value. Second, the investigations into the relationship between security investments and the organizational outcomes may assist the organizations in making judgmental resource allocation decisions. Third, research on the human factors influencing the security of EAIS, such as user-related practices, organizational culture, and training efficiency, would be welcome to develop more comprehensive strategies on security. Fourth, a study that considers the security risks of new technology, including quantum computing, powerful artificial intelligence, and future-generation blockchain applications, would assist organizations in being ready to face the future.

To sum up, though Electronic Accounting Information Systems promise enormous opportunities to improve the security of financial information due to automation, transparency, and high-quality controls, to achieve such opportunities, it is important to take into consideration various requirements and manage the critical challenges. Those organizations that apply holistic and risk-based thinking that incorporates technological solutions with organizational practices and human factors will be most likely to attain strong financial information security in an environment that becomes more digital and more threatening.

Bilibography list:

1/ Adil, D., Qassim, O. A., & Abbas, S. R. (2025). The Role of The Internal Control System in Light of The Electronic Operation of Accounting Data. *American Journal of Economics and Business Management*, *8*(3), 1257–1268. https://doi.org/10.31150/ajebm.v8i3.3410

2/ Ahmed, R. (2019). The impact of Accounting Information Systems' Quality on Accounting Information Quality. *Reform of Accounting and Auditing Systems- Reality & Requirements*.
https://www.researchgate.net/publication/330856912_The_impact_of_Accounting_Information_Systems

3/ al tarawneh , E. mahmoud , Alqaraleh , M. H., Ali , B. J. A., & Atta, A. A. B. (2023). The Impact of the Efficiency and Effectiveness of Electronic Accounting Information Systems on the Quality of Accounting Information. *Information Sciences Letters*, *12*(3), 1685–1692. https://doi.org/10.18576/isl/120352

4/ Barreto, A., Gomes, P., Patrícia Quesado, & O'Sullivan, S. (2025). Advancements in Management Accounting and Digital Technologies: A Systematic Literature Review. *Accounting Finance & Governance Review/Accounting Finance & Governance Review*, *34*. https://doi.org/10.52399/001c.137301

5/ Chandler, N. (2024). Shifting work competencies in an emerging economy: a comparison of accounting students' perceptions of demand and supply. *Higher Education, Skills and Work-Based Learning*, *15*(7). https://doi.org/10.1108/heswbl-08-2023-0213

6/ Cherian, S. (2025). *Cybersecurity Threats to Watch Out For in 2025 | Microminder Cybersecurity | Holistic Cybersecurity Services*. Microminder Cybersecurity. https://www.microminderc s.com/blog/cybersecurity-threats-to-watch-out-for

7/ Cong, L. W., & He, Z. (2018). *Blockchain Disruption and Smart Contracts*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764

8/ Daway, A. M., Wasan Mejbel Daway, Karrar Ali Zghair, & Hakeem Hammood Flayyih. (2025). The Impact of Digital Transformation of Accounting Information Systems on Enhancing the Effectiveness of Internal Control. *Journal of Lifestyle and SDGs Review*, *5*(3), e05572. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05572

9/ Fitriati, A., & Susanto, A. (2017). The improvement of accounting information system quality through internal control and effective top management support. Journal of Theoretical and Applied Information Technology, 95(19), 5003–5011.
https://www.researchgate.net/publication/320693408_The_accounting_information_system_quality_improvement_through_internal_control_and_top_management_support_effectiveness

10/ Hamdan, A., Khamis, R., Anasweh, M., Al-Hashimi, M., & Razzaque, A. (2019). IT Governance and Firm Performance: Empirical Study From Saudi Arabia. *SAGE Open*, *9*(2), 215824401984372. https://doi.org/10.1177/2158244019843721

11/ Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and Auditing with Blockchain Technology and Artificial Intelligence: a Literature Review. *International Journal of Accounting Information Systems*, *48*(1), 100598. sciencedirect. https://doi.org/10.1016/j.accinf.2022.100598

12/ Hyde, J. (2023, January). 3000% Increase in Deepfake Frauds! GMA.
https://www.gmal.co.uk/3000-increase-in-deepfake-frauds/

13/ Monteiro, A. P., Vale, J., Leite, E., Lis, M., & Kurowska-Pysz, J. (2022). The impact of information systems and non-financial information on company success. International

Journal of Accounting Information Systems, 45, 100557. https://doi.org/10.1016/j.accinf.2022.100557

14/ Nurul, N. (2025). The Role of Accounting Information Systems in Improving the Efficiency and Quality of Financial Reports. *Accounting Department, Muhammadiyah University of Palopo*. https://doi.org/10.2139/ssrn.5249175

15/ Nurwanah, A. (2024). Cybersecurity in Accounting Information Systems: Challenges and Solutions. *Advances in Applied Accounting Research*, *2*(3), 157–168. https://doi.org/10.60079/aaar.v2i3.336

16/ Secinaro, S., Dal Mas, F., Brescia, V., & Calandra, D. (2021). Blockchain in the accounting, auditing and accountability fields: a bibliometric and coding analysis. Accounting, Auditing & Accountability Journal, ahead-of-print(ahead-of-print). https://doi.org/10.1108/aaaj-10-2020-4987

17/ Tamzid. (2025). 500+ Ransomware Statistics (October-2025). Bright Defense. https://www.brightdefense.com/resources/ransomware-statistics/

18/ Zhu, L. (2022). Exploring the Significance of Digital Skills Training for Exploring the Significance of Digital Skills Training for Accountants Accountants. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=15205&context=dissertations