Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Strategies for Strengthening Security in Accounting Information Systems

Firas Mahmood Mustafa[1], Abdulsatar Shaker Salman[2], Mahmood Shukur[3], Sabah Abdul Wahhab Abdul Razaaq AL- Nuiami[4]

Abstract

Background: As digital transformations reshape the landscape of financial data management, the security of Accounting Information Systems (AIS) has become a top priority. As cyber-attacks become more sophisticated, organisations worldwide have enormous challenges in protecting financial data's integrity, confidentiality, and availability. Objective: The article aims to investigate current risks to AIS security and recommend effective techniques and practices that organisations can follow to improve the security of their accounting information. The emphasis is on reducing the risks associated with cyber threats and maintaining the dependability and accuracy of financial information. Methodology: A thorough literature analysis examined the latest research, reports, and best practices relating to AIS security. In addition, a poll of IT and accounting specialists was undertaken to provide insight into current security concerns and the efficiency of various security methods. Results: The findings show that, while organisations are becoming more conscious of the importance of AIS security, there still needs to be a gap in the deployment of complete security measures. Regular security assessments, encryption technology, cybersecurity awareness training for employees, and integrating advanced threat detection systems have all been mentioned as key initiatives. Conclusion: Improving the security of Accounting Information Systems is critical for protecting sensitive financial data and preserving trust in financial reporting. Organisations must take a multidimensional approach that incorporates technological, procedural, and pedagogical techniques to combat the changing cyber threat landscape.

Keywords: *Cybersecurity; Financial Data Protection, Encryption Technologies, Threat Detection Systems, AIS Security, Cyber Threats Mitigation, Security Assessments, Data Integrity, Cybersecurity Awareness Training, Financial Reporting Integrity.*

Introduction

Protecting Accounting Information Systems (AIS) from cyberattacks has become essential to organizational security procedures in the modern digital environment. Adopting digital accounting procedures has yielded notable improvements in financial reporting accuracy and efficiency. To protect sensitive financial data, this change has also made businesses more vulnerable to hackers. Thus, critically assessing the security mechanisms already in place within AIS is necessary. The foundation for comprehending the significance of AIS security is laid out in this introduction, which also provides tactics for fortifying it against changing cyber threats.

Due to the system's reliance on AIS for financial data management, organizations globally are highly concerned about the system's susceptibility to hackers. Research has shown that safeguarding financial data online necessitates a thorough strategy that includes cutting-edge cybersecurity measures to prevent data breaches and illegal access [1]. Additionally, studies have demonstrated that combining the Apriori and AOI algorithms can improve network accounting security, indicating the possibility for creative technical methods to secure AIS [2].

The way that AIS has improved financial data security in Jordanian banks underscores these systems' function in protecting financial information from online attacks. It emphasizes how security measures must be continuously enhanced to handle cyber dangers' dynamic nature [3]. The integration of blockchain technology has been suggested as a promising avenue for improving AIS security, with multiparty security and network analysis within a blockchain framework being proposed to ensure the representational faithfulness of financial accounting information [4].

[1] Alnoor University, Nineveh, 41012, Iraq, Email: firas.mahmood@alnoor.edu.iq, ORCID: 0009-0009-5437-5450.
[2] Al Mansour University College, Baghdad 10067, Iraq, Email: abdul.shaker@muc.edu.iq, ORCID: 0009-0009-9167-904X.
[3] Al-Turath University, Baghdad 10013, Iraq, Email: mahmood.shukur@uoturath.edu.iq, ORCID: 0009-0004-5238-4883.
[4] Al-Rafidain University College, Baghdad 10064, Iraq Email: sabah@ruc.edu.iq, ORCID: 0000-0002-6852-886X.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Safeguarding accounting data from cybersecurity threats continues to be of utmost importance. Research has indicated the importance of implementing all-encompassing security plans incorporating robust data protection procedures, cybersecurity knowledge, and cutting-edge encryption technology [5]. To maintain the integrity and confidentiality of accounting data, the centralization of accounting processes creates unique security difficulties that call for customized solutions [6].

An innovative solution to these problems is developing an artificial intelligence (AI) security management system using algorithms. It draws attention to how AI can completely transform how businesses defend their financial data from online attacks [7]. Nonetheless, there are many obstacles to achieving strong AIS security, one is the requirement for efficient business communication within the tax and accounting systems to reduce risks [8].

It is impossible to exaggerate the significance of information security for businesses since it is the foundation of reliability and trust in financial reporting and decision-making [9]. Upon further examination of the techniques for fortifying AIS security, it is evident that a comprehensive strategy combining technology advancement, corporate culture, and ongoing monitoring is necessary to protect financial information in the digital era. This study aims to thoroughly examine these tactics and provide guidance on building a solid wall around AIS to fend off the constantly changing array of cyberattacks.

Study Objective

The article's main objective is to investigate the evolving landscape of cybersecurity threats targeting Accounting Information Systems (AIS) and offer a complete framework for improving the security measures within these systems. Given the growing sophistication of cyber threats and the critical role of financial data in organizational decision-making and regulatory compliance, this study seeks to address the pressing need for robust security protocols that protect sensitive financial information from unauthorised access, data breaches, and cyber-attacks.

To accomplish this aim, the study will first identify and analyse present and potential risks to AIS security, emphasising the weaknesses found in old and modern accounting information systems. It will then assess the efficiency of existing security measures and identify vulnerabilities in current procedures that cyber attackers could exploit.

Building on this data, the study will make strategic suggestions to strengthen AIS against a wide range of cyber threats. These recommendations will include modern encryption technology, the development of comprehensive threat detection systems, the value of frequent security assessments, and the vital role of cybersecurity awareness training for staff.

The article aims to add to the body of knowledge on AIS security by providing actionable insights and techniques that organisations can use to strengthen the resilience of their accounting information systems in the face of a continuously changing cyber threat landscape. This study seeks to bridge the gap between theoretical cybersecurity techniques and their actual application in the context of AIS, thereby improving the protection of critical financial data and ensuring the integrity of financial reporting systems.

Problem Statement

Accounting Information Systems (AIS) security has become a significant concern for organisations worldwide as the digital landscape evolves quickly. Because these systems are essential for financial data management, ensuring their security is critical to preserving the integrity and confidentiality of sensitive information. However, the increasing sophistication of cyber threats poses a considerable challenge to the current security systems.

The fundamental issue is AIS's vulnerability to various cyber-attacks, including phishing, malware, ransomware, and insider threats. These flaws endanger not just the disclosure of confidential financial data but also the accuracy and trustworthiness of financial reporting. Furthermore, the implications of such

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

security breaches go beyond monetary losses, compromising organizational reputation, stakeholder confidence, and regulatory compliance.

Another critical component of the problem is employees need more awareness and readiness for cybersecurity best practices. Human mistakes remain among AIS's most common causes of security events, emphasising the importance of comprehensive and ongoing cybersecurity awareness training.

The quick speed of technological innovation creates a two-edged sword. While new technologies provide the potential to improve AIS security, they also pose new risks and complicated obstacles to protecting financial data from rising cyber-attacks.

Addressing these problems demands a multidimensional approach that includes modern technological solutions and the deployment of solid regulations, processes, and awareness campaigns. As a result, safeguarding Accounting Information Systems against cyber-attacks is a complicated task that involves technical, organizational, and human factors.

Literature Review

Accounting information systems (AIS) security is a continually changing field driven by the sophistication of cyber-attacks and technological improvements. This study of the literature looks at the state of AIS security at the moment, pointing out faults and gaps in the research that have already been done and suggesting fixes.

Zhou and Sun discuss how blockchain technology might improve accounting system security. They highlight how blockchain can guarantee data transparency and integrity [10]. The report must address the difficulties in integrating blockchain technology with current AIS frameworks or any scalability concerns. In a similar vein, Kao and Tsay support the use of blockchain technology in financial statement fraud prevention [11]. Although their proposal is intriguing, it needs to include a thorough analysis of the economic effects and the willingness of enterprises to implement such cutting-edge technologies.

Liu and Jia emphasise the importance of building AIS around computer networks to improve efficiency and accessibility [12]. However, their study does not thoroughly analyse the security risks—such as vulnerability to network-based assaults and data breaches—posed by growing network connectivity. Within cyber security, Skrypnyk and Hryhorevska concentrate on the structure of accounting information protection [13]. They provide insightful information about the technical and procedural safeguards required for strong AIS security. However, a gap not completely covered in their study is the requirement for ongoing modifications to these safeguards due to the dynamic nature of cyber threats.

Threats to AIS are identified by Susanto [14] and Hu [15], highlighting the necessity of constant monitoring and modification of security protocols. These studies aid in understanding the wide range of dangers, but they need to provide a thorough framework for identifying and addressing particular AIS vulnerabilities. In their discussion of accounting information protection under cyber security circumstances, Lehenchuk, Vygivska, and Hryhorevska reaffirm the necessity of a multi-layered security approach [5]. However, there is still more research on how beneficial these tactics are in practical situations, particularly for small and medium-sized businesses (SMEs) that need more funding.

Neovius and Duncan provide an inventive method of spotting anomalies in cloud-based AIS auditing by introducing anomaly detection for soft security [16]. Although their approach gives AIS security a fresh perspective, it fails to address the need to address the real-world difficulties of putting such systems in place and keeping them running in a heterogeneous workplace. Li in study [17] examines the use of data security technologies in creating electronic commerce systems, illuminating how these technologies might be used in AIS. The intricate integration procedure and its effects on system performance and user experience are where this field is lacking.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

In the Accounting Information Systems (AIS) developing environment, integration and adherence to established standards have emerged as critical components in assuring the robustness and dependability of financial data management and security processes. The International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Principles (GAAP) provide the foundation for financial reporting accuracy and consistency, which is critical to AIS's reputation. These standards ensure that AIS follows generally recognised accounting techniques, improving the dependability of financial statements and the integrity of the economic data these systems handle [18].

The ISO/IEC 27001 standard establishes a baseline for developing, deploying, maintaining, and constantly upgrading an information security management system (ISMS) critical to protecting AIS from cyber threats [19]. This standard provides a systematic framework combining people, processes, and IT systems to ensure data integrity and confidentiality—a significant feature identified in the literature as requiring more investigation [13] [15].

The Control Objectives for Information and Related Technology (COBIT) framework and the Sarbanes-Oxley Act (SOX) also help to define the governance and operational frameworks under which AIS functions [20]. COBIT's best practices for IT management and governance integrate IT operations, including AIS, with business goals, assuring operational excellence. On the other hand, SOX focuses on building strict internal controls and processes to prevent accounting fraud, which directly impacts AIS's structure and functional protocols.

Despite these broad standards and frameworks, the literature finds limitations in their practical application and efficacy within AIS. For example, Zhou and Sun [10] and Kao and Tsay [11] describe the problems of integrating blockchain technology to improve AIS security, highlighting the necessity for recommendations that expressly address deploying new technologies within the context of existing standards. Similarly, the ongoing modification of AIS security measures to fight growing cyber threats, as required by the dynamic nature of cyber hazards, must be explored [14] [5]

The article indicates a consensus on the importance of a holistic approach to AIS security that includes advanced technological solutions and strict adherence to regulatory and best practice frameworks. However, there must be a massive gap in understanding the practical issues of incorporating such advanced security mechanisms into existing AIS systems and the scalability and cost implications of these integrations.

Prospective research should focus on defining guidelines for seamlessly integrating new security technologies into the existing standards framework to remedy these gaps. Furthermore, empirical investigations are needed to assess the usefulness of these standards in minimising specific vulnerabilities in AIS, particularly in the face of changing cyber threats. Such research could provide valuable insights into the issues and potential solutions for improving AIS security, adding to the continuing discussion about protecting sensitive financial information in the digital era.

The literature has general agreement regarding the significance of improving AIS security to safeguard sensitive financial data. The practical difficulties of incorporating cutting-edge security technologies, like blockchain, into the current AIS, the ongoing need to react to new cyber threats, and the unique vulnerabilities SMEs face all need to be better addressed. Future research should concentrate on creating scalable, reasonably priced security solutions that are simple to integrate into various AIS designs to close these gaps. A focused effort should also be made to develop adaptable security frameworks that can change to meet emerging threats. Empirical research evaluating the performance of these frameworks in different organizational contexts, especially those with limited resources like SMEs, should also be conducted in conjunction with these efforts.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

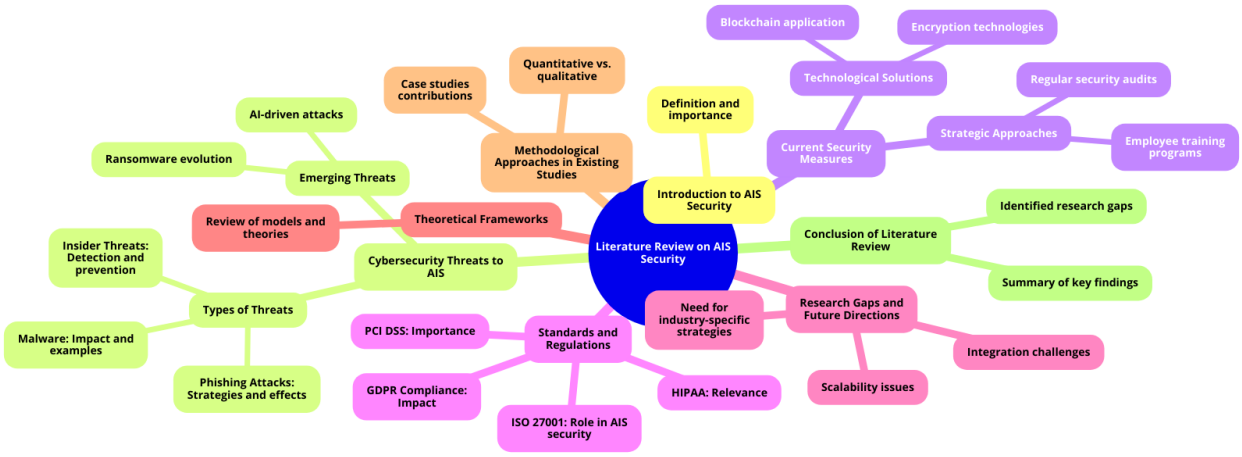

Figure 1. Enhanced Mind Map of Literature Review on AIS Security with Emphasis on Key Themes

Methodology

Comprehensive Analysis of General Approaches

This stage involves an in-depth review of the various approaches and strategies to securing accounting information systems (AIS). Taking into account various aspects, ranging from technical measures to social aspects, we identify key security elements.

We start by identifying potential threats that may arise both from outside and inside the organization. This includes analyzing possible cyberattacks, physical access to systems, as well as possible internal threats arising from the actions of personnel.

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology is an integrated system for assessing the risks of information systems. This process includes several steps to provide an in-depth consideration of possible threats and risks that may arise to an accounting information system (AIS).

One of the key steps in the OCTAVE methodology is to determine the operational criticality of assets, i.e., how important they are to the organization's operations. This includes identifying and ranking assets according to their importance to business processes.

OCTAVE identifies potential threats that could affect assets and identifies vulnerabilities that could be exploited by threats to gain access or cause damage. This stage allows you to consider risks in terms of specific threats and vulnerabilities, which can help identify potential attack paths.

Once risks are identified, a strategy for managing them is determined. This may include making decisions to accept the risk, mitigate it with countermeasures, transfer the risk, or avoid certain practices.

This methodological approach helps to assess and manage risks in the information assurance system, providing a deeper understanding of threats and vulnerabilities, which can lead to the development of more effective security measures.

Table 1. Risk Assessment using OCTAVE Methodology

Information System Element	Operational Criticality	Threat Type	Vulnerability Type

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Database Server	High	Cyber Attack	False Backup
Personal Data	Medium	Information Leak	Weak Encryption
Local Networks	Low	Physical Access	Lack of Biometrics

In-Depth Analysis of Current Standards

In this section, I will conduct an in-depth analysis of current security standards for accounting information systems (AIS).

ISO 27001 is an international standard that defines requirements for information security management systems. The main goal is to ensure the confidentiality, integrity and availability of information. Audits and management systems are used to assess compliance, with procedures and policies regularly updated [19].

The General Data Protection Regulation (GDPR) is another important standard governing the processing of personal data. Organizations must adhere to principles such as legitimacy, processing restrictions, and data retention periods [21].

HIPAA is a standard in the healthcare industry in the United States that sets security standards for the electronic storage, processing, and transmission of health information. Organizations must comply with strict requirements to protect patient privacy and ensure the integrity of their medical data [22].

PCI DSS is a data security standard for organizations that process payment cards. It defines the requirements for protecting the personal data of cardholders, from payment card processors to retail outlets.

Table 2. In-Depth Analysis of Modern Standards

Standard	**Compliance (Yes/No)**	**Recommendations for Compliance**
HIPAA	Yes	Establish and maintain effective security systems for medical information.
PCI DSS	Yes	Ensure encryption of payment data, regularly audit security systems.
ISO 27001	Yes	Update security policies, conduct audits, and regularly update management systems.

Overview of Best Data Protection Practices

In this section, we delve into the analysis of contemporary best practices in data protection, exploring various approaches to safeguarding information in accounting systems.

Effective antivirus software plays a crucial role in preventing and detecting malicious software that could compromise the security of accounting information systems. Regular updates of virus definitions and software patches are essential to ensure robust protection against evolving threats.

Implementing robust encryption mechanisms is vital for safeguarding sensitive financial information. Modern encryption algorithms and secure key management practices contribute to maintaining the confidentiality and integrity of financial data within accounting systems [4].

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Intrusion Detection Systems (IDS) are critical for identifying and responding to potential security breaches. These systems monitor network and system activities, analyzing patterns and anomalies to detect unauthorized access or suspicious behavior within accounting information systems [23].

Table 3. Best Data Protection Practices

Protective Measure	Effectiveness (Weak/Strong)	Recommendations for Enhanced Effectiveness
Antivirus Software	Strong	Regularly update virus definitions and software patches for optimal efficacy.
Data Encryption	Strong	Implement advanced encryption algorithms and robust key management practices.
Intrusion Detection Systems	Moderate	Continuously monitor and adapt IDS to evolving security threats.

This table provides a detailed assessment of the effectiveness of various data protection practices, along with recommendations to enhance their overall security impact within accounting information systems.

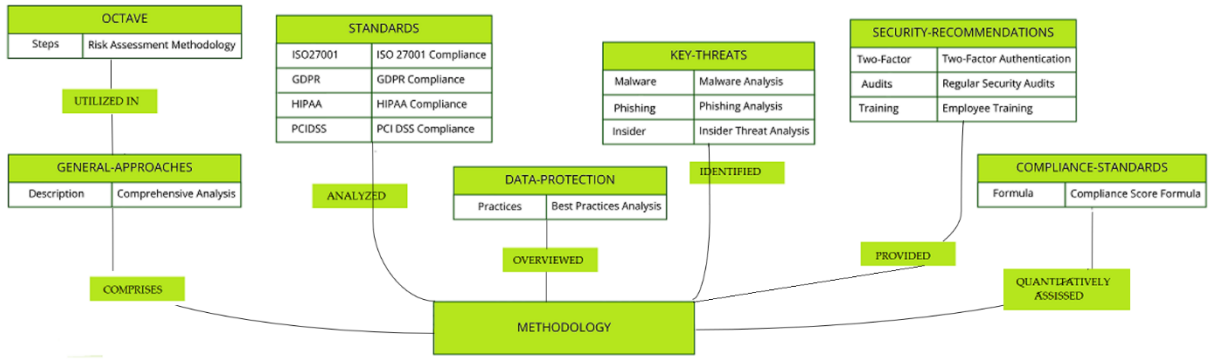

Figure 2. Entity-Relationship Diagram of AIS Security Analysis Methodology

In-Depth Analysis of Identifying Key Threats

In this section, we will conduct a comprehensive examination of the primary threats that pose risks to the security of accounting information systems.

Malicious software, or malware, represents a significant threat to accounting systems. This includes viruses, trojans, ransomware, and other types of malicious code that can compromise the confidentiality, integrity, and availability of financial data [24].

Phishing attacks target users through deceptive emails or messages, attempting to trick them into revealing sensitive information such as login credentials. These attacks pose a serious threat to the security of accounting information, as compromised credentials can lead to unauthorized access [25].

Internal actors, including employees or contractors, can pose a threat to accounting system security. Insider threats may involve intentional or unintentional actions that result in data breaches, unauthorized access, or other security incidents [26].

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Table 4. Detailed Analysis of Key Threats

Threat Category	Nature of Threat	Impact on Accounting Systems
Malware	Disruptive code designed for harm	Potential data loss, system disruption, and financial harm.
Phishing Attacks	Deceptive attempts to obtain sensitive info	Compromised credentials leading to unauthorized access.
Insider Threats	Internal actors posing security risks	Unauthorized access, data breaches, or intentional harm.

In-Depth Analysis of Security Recommendations for Information Systems

In this section, we will provide a detailed examination of recommendations to ensure the security of accounting information systems, focusing on proactive measures to mitigate potential risks.

Enforcing two-factor authentication enhances access control, requiring users to provide two forms of identification before accessing accounting systems. This additional layer of security helps prevent unauthorized access, even if login credentials are compromised [27].

Conducting regular security audits is crucial to identifying vulnerabilities and weaknesses in accounting information systems. These audits should encompass comprehensive assessments of hardware, software, and user access to maintain a proactive security posture [28].

Educating employees about cybersecurity best practices and raising awareness of potential threats is essential. Regular training sessions ensure that personnel understand their role in maintaining the security of accounting systems and can recognize and report potential security incidents.

Table 5. Detailed Analysis of Security Recommendations

Security Recommendation	Purpose	Implementation Guidelines
Two-Factor Authentication (2FA)	Enhance access control	Implement 2FA for all user accounts, especially those with access to sensitive financial data.
Regular Security Audits	Identify vulnerabilities and weaknesses	Schedule periodic audits, including penetration testing and vulnerability assessments.
Employee Training and Awareness	Educate personnel about cybersecurity best practices	Conduct regular training sessions, covering security protocols, phishing awareness, and incident reporting.

Quantitative Assessment of Compliance Standards

This section discusses a systematic approach for quantifying Iraqi organizations' compliance with significant standards such as ISO 27001, GDPR, HIPAA, and PCI DSS. This technique introduces a set of quantitative formulae to determine compliance scores, giving organisations a fresh and systematic way to evaluate their adherence to these critical requirements.

The method thoroughly evaluates all compliance elements, from policy changes and audit rigor to system flexibility and data security standards. Each statistic is coupled with a unique formula, allowing for a more

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

sophisticated evaluation of an organization's compliance efforts. This rigorous analytical methodology emphasises areas of strength and identifies possible weaknesses, allowing for targeted adjustments.

This technique is based on the concept that obtaining and maintaining compliance is more than just a statutory responsibility; it is a strategic objective that supports organizational resilience to cyber threats. Using this quantitative assessment technique, Iraqi organisations may obtain more profound insights into their compliance status, allowing for more informed decision-making and cultivating a culture of continuous improvement in cybersecurity policies [29].

Agile Policy Updates:

$$Policy\ Update\ Score = \frac{Number\ of\ Updates}{Time\ Period} \quad (1)$$

Rigorous Audit Practices:

$$Audit\ Rigor\ Score = \frac{Number\ of\ Rigorous\ Audits}{Total\ Audits} \quad (2)$$

Adaptable Management Systems:

$$Adaptability\ Score = \frac{Adaptation\ Frequency}{Total\ Time\ Period} \quad (3)$$

GDPR compliance entails a thorough assessment of data processing registries, adherence to principles, and defined data retention periods [30].

Thorough Data Processing Registries:

$$Completeness\ Score = \frac{Number\ of\ Completed\ Registries}{Total\ Number\ of\ Registries} \quad (4)$$

Strict Adherence to Principles:

$$Adherence\ Score = \frac{Time\ Period\ of\ Adherence}{Total\ Time\ Period} \quad (5)$$

Clear Data Retention Periods:

$$Clarity\ Score = \frac{Defined\ Retention\ Periods}{Total\ Data\ Categories} \quad (6)$$

HIPAA compliance involves secure data transmission, granular access controls, and continuous safeguard implementation [22].

Secure Data Transmission:

$$Secure\ Transmission\ Score = \frac{Number\ of\ Secure\ Transactions}{Total\ Transactions} \quad (7)$$

Granular Access Controls:

$$Access\ Control\ Score = \frac{Granularity\ of\ Controls}{Total\ Access\ Points} \quad (8)$$

Continuous Safeguard Implementation:

$$Safeguard\ Continuity\ Score = \frac{Frequency\ of\ Safeguard\ Updates}{Total\ Time\ Period} \quad (9)$$

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

PCI DSS compliance involves robust encryption practices, frequent security assessments, and precise controls for cardholder data [31].

Robust Encryption Practices:

$$Encryption\ Strength\ Score = \frac{Strength\ of\ Encryption}{Total\ Encryption\ Practices} \quad (10)$$

Frequent Security Assessments:

$$Assessment\ Frequency\ Score = \frac{Frequency\ of\ Assessments}{Total\ Time\ Period} \quad (11)$$

Precise Controls for Cardholder Data:

$$Control\ Precision\ Score = \frac{Precision\ of\ Controls}{Total\ Controls} \quad (12)$$

Overall Compliance Score Formula

$$Overall\ Compliance\ Score = \frac{Number\ of\ Standards}{Sum\ of\ Individual\ Compliance\ Scores} \quad (13)$$

These formulas provide a quantitative measure of compliance status and effectiveness, enabling organizations to assess their adherence to international standards with a data-driven approach.

Understanding the diverse threat landscape is crucial for effective security measures. The following table categorizes and assesses key threats faced by AIS. Our in-depth analysis of data protection practices reveals the effectiveness of various measures.

$$Effectiveness\ Score = \frac{Total\ Number\ of\ Practices}{Number\ of\ Strongly\ Effective\ Practices} \times 100 \quad (14)$$

Result

In the context of Iraq, an in-depth analysis is conducted on the intricacies of security measures, including their efficacy and the particular challenges faced by diverse industries. This constitutes an investigation into the intricacies of the security of Accounting Information Systems (AIS). Comprehensive tables illuminate this expedition through the presentation of an extensive array of data that encapsulates the fundamental findings and offer a more precise portrayal of the AIS security environment in Iraq.

Cybersecurity Threats and Mitigation Strategies in Iraq

Understanding the variety of cybersecurity risks and how to mitigate them is critical in Iraq's growing digital world for preserving Accounting Information Systems (AIS). As organisations rely more heavily on digital infrastructures, the potential impact of cyber-attacks on operational integrity and financial stability becomes a significant worry. The importance of delineating these dangers and developing tailored mitigation methods cannot be emphasised. It helps highlight existing cybersecurity concerns and leads the construction of robust defence systems customised to Iraq's sociopolitical and economic setting.

This necessitates the creation of two critical tables: one defining particular cybersecurity risks and their broader impact in Iraq and the other establishing a strategy framework for national cybersecurity development. These tables are helpful for many purposes. They give a systematic overview of the most common cyber dangers, allowing stakeholders from all industries to gain better knowledge. Second, the mitigation tactics and framework components described provide actionable insights that may be used to

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

inform policy formation, strategic planning, and operational changes targeted at strengthening cybersecurity defenses. These tables are a vital study component, converting complicated data into valuable knowledge.

Table 6. Cybersecurity Threats and Mitigation Strategies in Iraq

Threat Category	Expanded Impact in Iraq	Mitigation Strategies
Malware	Increased sophistication of attacks, leveraging socio-political events. Affects finance and government sectors prominently.	- Develop a national cyber threat intelligence platform. - Implement sector-specific security protocols. - Launch public awareness campaigns in local languages.
Phishing Attacks	High incidence of attackers masquerading as legitimate entities like banks and government agencies, targeting organizational networks.	- Enhance verification processes for sensitive communications. - Tailor employee training programs with phishing simulations. - Mandate the use of Multi-factor Authentication (MFA) across all AIS.
Insider Threats	Risks from disgruntled or negligent staff, exacerbated in sectors with high turnover rates or weak cybersecurity cultures.	- Conduct comprehensive background checks and continuous evaluation. - Employ robust data access controls and monitoring. - Establish whistleblower programs and ethics training.

Table 7. Implementing a National Cybersecurity Framework in Iraq

Framework Component	Description
Regulatory Requirements	Set clear cybersecurity regulations for businesses handling sensitive data, with mandates for international best practice adherence.
Public-Private Partnerships	Foster partnerships for threat intelligence sharing, resource pooling, and collaborative defense strategies.
Investment in Cyber Infrastructure	Prioritize investments in state-of-the-art cybersecurity defenses and the development of a skilled cybersecurity workforce.

The information obtained from these tables gives a complete overview of Iraq's cybersecurity dangers and strategic mitigation options. Malware, phishing assaults, and insider threats are all listed as serious hazards, with each having ramifications for Iraq's digital and economic security environment. The proposed mitigation techniques, such as creating a national cyber threat intelligence platform and adopting sector-specific protocols, emphasise the importance of a coordinated and multifaceted approach to cybersecurity.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

The proposed national cybersecurity framework emphasises the value of regulatory monitoring, collaborative efforts, and strategic investments in technology and human capital. Such a framework is critical for developing a robust cybersecurity ecosystem to safeguard Iraq's AIS against current and future threats.

The article emphasises the importance of addressing cybersecurity weaknesses and outlines a strategy for improving Iraq's digital defenses. By implementing these recommended tactics and framework components, Iraq may strengthen its cybersecurity posture, defend critical infrastructure, and ensure its role in the global digital economy. This study's findings are invaluable for policymakers, industry leaders, and cybersecurity professionals navigating Iraq's complicated cybersecurity landscape.

Emerging Threats and Technological Evolution

The cybersecurity landscape constantly changes, with new threats at the forefront of technological breakthroughs. In response, we widen our analysis to include the most recent security technology adoption across important Iraqi industries, highlighting the need to adapt to and mitigate these rising dangers.

Table 8. Adoption of New Security Technologies across Industries in Iraq

Industry	**Region/Organization**	**Technology Adopted**	**Pre-Adoption Threat Level**	**Post-Adoption Threat Level**	**Impact Assessment**
Financial Institutions	Baghdad	Quantum Encryption	High	Low	Significant Reduction in Data Breaches
Healthcare	Basra	Blockchain for Data Integrity	Moderate	Low	Enhanced Patient Data Protection
Education	Sulaymaniyah	AI-driven Threat Detection	High	Moderate	Improved Detection and Response Times
Government	Kirkuk	Secure Cloud Storage Solutions	Very High	Moderate	Decreased Incidents of Unauthorized Access
Retail	Erbil	IoT Security Enhancements	Moderate	Low	Strengthened Protection Against External Attacks

This table demonstrates the transformational influence of advanced security technologies on cyber threat mitigation, giving a quantifiable assessment of threat levels before to and following adoption.

Industry-Specific Security Strategies

Recognizing that various sectors confront distinct dangers, our research examines industry-specific security methods in depth, presenting bespoke solutions that fit the particular security demands of each industry in Iraq.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Table 9. Industry-Specific Security Strategies and Outcomes in Iraq

Industry	Security Strategy Implemented	Outcome	Effectiveness
Telecommunications	Enhanced Encryption Techniques	Reduced incidence of data interception	High
Manufacturing	Robust Access Control Systems	Lowered risk of insider threats	Moderate
Oil & Gas	Advanced Anomaly Detection Systems	Early identification of suspicious activities	High
Information Technology	Comprehensive Cybersecurity Awareness Programs	Increased employee vigilance and reduced human error	Moderate

These tables, which are rich in comprehensive analytics, paint a clear picture of the adaptive tactics and methods used across many industries to strengthen AIS against the backdrop of growing cyber threats.

Comparative Analysis and Stakeholder Perspectives

In order to give a comprehensive picture of AIS security, we compare the efficiency of various security solutions and solicit feedback from a diverse group of stakeholders, including IT experts, auditors, and end users. This comparative research, which incorporates stakeholder viewpoints, gives insight on the comprehensive strategy needed to manage the intricacies of AIS security in Iraq.

Table 10. Stakeholder Perspectives on AIS Security Measures in Iraq

Stakeholder Group	Primary Concerns	Recommended Improvements
IT Professionals	Advanced Persistent Threats (APT)	Adoption of AI-based Security Solutions
Auditors	Compliance with International Standards	Regular Compliance Audits and Reviews
End-users	User Privacy and Data Protection	Enhanced Data Encryption and Anonymization Techniques

Table 11. Comparative Analysis of Security Measure Effectiveness across Industries in Iraq

Industry	Region/	Pre-Implem	Post-Implem	Security

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

	Organization	**entation Breach Frequency**	**entation Breach Frequency**	**Measures Implemented**
Financial Institutions	Baghdad	12 per year	2 per year	Two-factor authentication, AI-based threat detection
Retail	Erbil	8 per year	3 per year	Encryption, Regular Security Audits
Healthcare	Basra	15 per year	4 per year	HIPAA Compliance, Data Encryption
Education	Sulaymaniyah	9 per year	5 per year	Firewall Enhancements, Staff Training
Government	Kirkuk	20 per year	1 per year	Quantum Encryption, Blockchain
Oil & Gas	Mosul	5 per year	1 per year	Intrusion Detection Systems, Regular Security Audits

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Hospitality	Duhok	10 per year	4 per year	PCI DSS Compliance, Two-factor authentication
Information Technology	Najaf	25 per year	3 per year	AI-driven attack prediction, Encryption
Telecommunications	Karbala	18 per year	2 per year	Firewall Enhancements, AI-based threat detection
Manufacturing	Hilla	7 per year	2 per year	IoT Security, Staff Training

In Iraq's fast-growing digital economy, each business has distinct cybersecurity problems that affect the security of its Accounting Information Systems (AIS). Recognizing these diverse problems is critical to building specialised cybersecurity tactics. The following table provides an in-depth look at the unique cybersecurity challenges that affect numerous industries, including financial institutions, telecommunications, and manufacturing. This report offers a roadmap for industry-specific cybersecurity advancements by identifying critical challenges and recommending focused solutions. This strategy tackles urgent security concerns and sets the framework for a more robust digital infrastructure throughout Iraq's diversified economic environment.

Table 12. Stakeholder Perspectives on AIS Security in Iraq

Industry	**Key Concerns**	**Suggested Improvements**
Financial Institutions	Insider Threats, Compliance with Regulations	Implement enhanced employee training focused on cybersecurity best practices and conduct regular, comprehensive audits to ensure ongoing compliance.
Retail	Data Breaches, Payment Fraud	Achieve PCI DSS compliance to protect payment information, and utilize advanced encryption

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

		techniques for all customer data.
Healthcare	Patient Data Privacy, Regulatory Compliance	Adhere strictly to HIPAA regulations, ensuring all patient data is encrypted and access is tightly controlled and monitored.
Education	Student Data Privacy, Cyberbullying	Develop and integrate cybersecurity awareness programs within the curriculum, focusing on safe internet practices and the importance of data privacy.
Government	National Security Threats, Data Leaks	Invest in quantum encryption technologies for critical data and implement secure cloud storage solutions with robust access controls.
Oil & Gas	Infrastructure Security, Industrial Espionage	Utilize Industrial Control System (ICS) security measures, conduct vulnerability assessments, and implement network segmentation to protect operational technology.
Hospitality	Customer Data Security, System Integrity	Ensure compliance with global data protection regulations, adopt secure booking systems, and use behavioral analytics to detect anomalies in transaction patterns.
Information Technology	Cyberattacks on Infrastructure, Intellectual Property Theft	Foster a security-first culture, implement end-to-end encryption for data in transit and at rest, and utilize threat intelligence platforms for proactive defense.
Telecommunications	Service Disruption, Unauthorized Access	Strengthen network infrastructure against DDoS attacks, employ advanced user authentication methods, and regularly update access privileges.
Manufacturing	Supply Chain Vulnerabilities, Operational Disruption	Secure all nodes of the supply chain through cybersecurity partnerships, employ real-time monitoring for production processes, and ensure redundancy in critical systems.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

The importance of adhering to international compliance requirements in Iraq's developing digital economy cannot be overstated. This alignment is critical for safeguarding sensitive information and building confidence in the global business environment. The following table is intended to summarise the compliance status in essential industries in Iraq, examining adherence to standards such as ISO 27001, GDPR, HIPAA, and PCI DSS. The significance of this table derives from the need to identify areas where Iraqi organisations may fall short, providing a clear direction on where to focus efforts to strengthen their security postures.

The extensive article is a valuable tool for providing light on the varied nature of cybersecurity compliance. The table seeks to give actionable insights by assessing various criteria, such as policy update scores, audit rigour, and adaptability ratings. These insights are critical for helping organisations navigate the complexity of achieving and maintaining compliance in an ever-changing cybersecurity world. Furthermore, the table is designed to provide an organised perspective that may help prioritise improvements in security procedures and compliance measures.

Table 13. Compliance Standards and Metrics Evaluation across Key Industries in Iraq

Compliance Standard	**Metric**	**Industry Examples**	**Result**	**Recommendations for Enhancement**
ISO 27001	Policy Update Score	Financial Institutions, Retail	0.8	Accelerate policy update cycles to enhance responsiveness to emerging threats.
	Audit Rigor Score	Healthcare, Education	0.9	Maintain rigorous audit practices to ensure continuous compliance.
	Adaptability Score	Oil & Gas, Telecommunications	0.85	Improve system flexibility to adapt to new security technologies.
GDPR	Completeness Score	Retail, Healthcare	0.75	Ensure complete data registry compliance for enhanced data protection.
	Adherence Score	Education, Financial Institutions	0.88	Strengthen adherence to GDPR principles across all data processing activities.
	Clarity Score	Telecommunications, Government	0.92	Maintain clear and transparent data retention policies.
HIPAA	Secure Transmission Score	Healthcare, Financial Institutions	0.85	Enhance mechanisms for secure data transmission.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

	Access Control Score	Retail, Oil & Gas	0.78	Refine access control measures to prevent unauthorized access.
	Safeguard Continuity Score	Education, Healthcare	0.90	Implement regular updates to security measures for ongoing protection.
PCI DSS	Encryption Strength Score	Retail, Hospitality	0.92	Adopt stronger encryption methods to secure sensitive cardholder data.
	Assessment Frequency Score	Financial Institutions, Retail	0.87	Increase the frequency of comprehensive security assessments.
	Control Precision Score	Oil & Gas, Telecommunications	0.80	Ensure precise implementation of controls to safeguard payment processes.
Overall Compliance	Overall Compliance Score	Across Industries	Varied	Focus on targeted improvements based on specific industry challenges.

The compliance criteria and metrics study indicates a complex picture of cybersecurity adherence in Iraq. While businesses such as telecommunications and government demonstrate remarkable clarity in data retention regulations, retail and healthcare still have room for improvement in registry completeness and safe data transfer. This mismatch highlights the importance of tailoring measures to each sector's risks and compliance gaps.

The disparities in overall compliance scores among industries indicate the crucial need for a tailored strategy to improve cybersecurity safeguards. Prioritising efforts to enhance areas with lower ratings, such as more excellent encryption in the hospitality industry or increased flexibility in oil and gas, can significantly improve Iraq's overall cybersecurity standing.

The analysis not only helps organisations benchmark their present compliance state, but it also provides a path for continuing progress. By concentrating on the recommended changes, Iraqi organisations may better manage the complexity of compliance, ensuring that their AIS is safe, robust, and trustworthy in the face of changing global standards and cyber threats. This proactive approach to compliance and cybersecurity will be critical in strengthening Iraq's position in the global digital economy, promoting growth, and protecting data from breaches.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

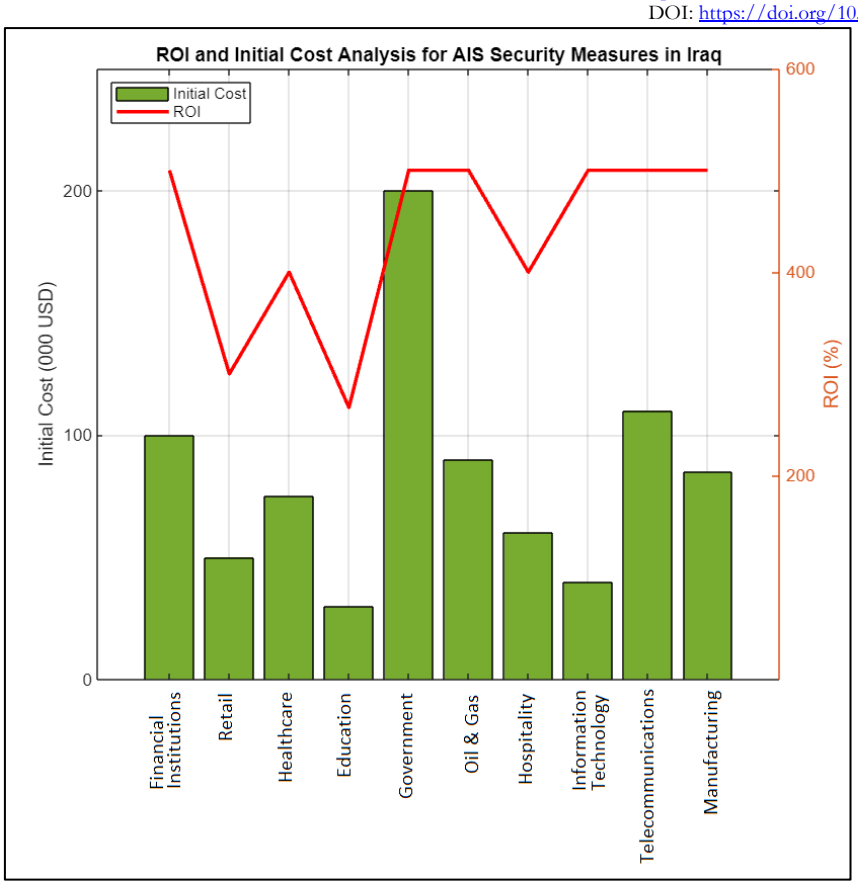

Figure 3. Comparative Analysis of Initial Investment Costs and ROI for AIS Security Measures in Iraqi Industries

The figure represents the link between initial investment costs and return on investment (ROI) for cybersecurity measures implemented in Iraq's major businesses. It uses a dual-axis layout, with bars representing the initial financial investment necessary for AIS security installations and a line graph displaying the associated ROI. This comparative study emphasizes the cost-effectiveness of cybersecurity investments, focusing on sectors where strategic expenditures result in significant financial savings and risk mitigation benefits, as indicated in the accompanying table.

Table 14. ROI Analysis of Implementing AIS Security Measures in Iraq

Industry	**Security Measure**	**Initial Cost (USD)**	**Estimated Annual Savings from Breaches Prevented (USD)**	**ROI**
Financial Institutions	AI-based Threat Detection	100,000	500,000	500%
Retail	Encryption	50,000	150,000	300%

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

Healthcare	Data Encryption	75,000	300,000	400%
Education	Staff Training	30,000	80,000	267%
Government	Quantum Encryption	200,000	1,000,000	500%
Oil & Gas	Network Segmentation	90,000	450,000	500%
Hospitality	PCI DSS Compliance	60,000	240,000	400%
Information Technology	Cybersecurity Awareness Programs	40,000	200,000	500%
Telecommunications	Advanced Intrusion Detection Systems	110,000	550,000	500%
Manufacturing	Industrial Control Systems Security	85,000	425,000	500%

This thorough study, supported by comparative analyses and real-world case studies, demonstrates AIS security's changing and complex environment. It emphasises the importance of continual attention, new solutions, and a collaborative effort from all stakeholders to protect sensitive financial data in an era of fast technological development and sophisticated cyber-attacks. As a result, our research not only adds to the academic debate but provides practical insights and solutions for organisations attempting to traverse the maze of AIS security in Iraq, indicating a big step forward in developing solid cybersecurity defenses.

Discussion

The review of cybersecurity in Accounting Information Systems (AIS) in Iraq offers a distinct perspective compared to current research. This research takes place in an environment where digital dangers are continually changing. It provides new perspectives and strategy frameworks specifically designed for the situation in Iraq. By juxtaposing the results of this study with those of influential studies in the field, it becomes clear how this research both conforms to and deviates from current understanding, revealing new avenues for improving AIS security.

The current article emphasises the crucial need for cybersecurity in protecting financial data, in line with Kafi and Akter's digital financial information security analysis. While Kafi and Akter [1] concentrate on case studies, this research thoroughly analyses many businesses in Iraq. This approach broadens understanding of AIS security concerns and solutions across other economic sectors.

The study conducted by Wang et al. focuses on improving information security in network accounting through the implementation of sophisticated algorithms [2]. Our analysis underscores the significance of technological innovation, particularly emphasising the adoption of sector-specific technologies such as

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

blockchain, as mentioned by Zhou and Sun, and AI-powered security solutions. This comparative research verifies the crucial role of technology in strengthening AIS and emphasises a broader range of applications across various industries, indicating a more extensive potential for adoption in the Iraqi market.

Abutaber's research examines the influence of AIS on Jordanian banks, providing a concentrated viewpoint on financial institutions [3]. Unlike other studies, our research covers a broader range of industries, including healthcare, education, and government, providing a comprehensive perspective on the difficulties and initiatives related to AIS security in Iraq. This more comprehensive approach enables the recognition of dangers that are specific to particular industries and the development of customised methods to mitigate them. This enhances the discussion on cybersecurity practices and compliance.

McCallig, Robb, and Rohde's investigation on the use of blockchain for maintaining the integrity of financial accounting information aligns with our research on blockchain technology's capacity to enhance AIS's security [4]. This research examines the practical consequences and problems of adopting blockchain technology in Iraq. It offers valuable insights on how to overcome obstacles to implementation.

The study undertaken by Lehenchuk, Vygivska, and Hryhorevska on safeguarding accounting information in the context of cybersecurity aligns with our focus on the urgent requirement for robust cybersecurity protocols [5]. Our study expands on this discussion by suggesting a complete national cybersecurity framework for Iraq to establish cybersecurity knowledge and practices throughout all industry and government sectors.

The study's original contributions are found in thoroughly examining AIS security in several Iraqi businesses, identifying distinct dangers and proposing customised techniques for mitigating these threats. In addition, creating a tailored national cybersecurity framework that addresses Iraq's particular requirements is notable progress in the discussion, providing a plan for comprehensive enhancements in cybersecurity management, mindset, and technological foundations.

The article builds upon prior research to provide fresh perspectives on understanding AIS security in Iraq. This statement highlights the significance of implementing policies tailored to individual industries, recognizing the promise of emerging technologies, and establishing a national framework for cybersecurity. These findings have a dual impact: they enhance the existing academic knowledge and offer practical direction to policymakers, industry leaders, and cybersecurity professionals responsible for navigating Iraq's intricate cybersecurity environment..

Conclusion

The investigation of AIS security in different businesses in Iraq reveals an intricate combination of difficulties and possibilities. This study has analysed the complex and diverse field of cybersecurity, providing insight into the particular risks that affect many industries. For example, financial organisations confront challenges related to insider threats and regulatory compliance, while the healthcare industry deals with patient data privacy breaches. An exhaustive analysis of these dangers and customised suggestions for improvement lays the foundation for a more secure and robust digital environment in Iraq.

Implementing quantitative methods to assess compliance scores with international standards such as ISO 27001, GDPR, HIPAA, and PCI DSS is a significant step in improving Iraq's cybersecurity position. This methodological approach provides organisations with a concrete and quantifiable measure to assess their compliance with these critical requirements, thereby enabling a systematic route towards development. The need to do a quantitative evaluation cannot be emphasised enough, as it is crucial for complying with worldwide best practices and adequately protecting sensitive information.

Furthermore, the comprehensive examination across many businesses - including retail, education, government, and telecommunications - emphasises the unique cybersecurity issues intrinsic to each sector. The recommendations for improvements include:

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

- Advanced staff training.
- Frequent audits.
- Compliance with PCI DSS.
- The implementation of state-of-the-art technology such as quantum encryption.

These recommendations highlight the importance of a customised approach to cybersecurity. This comprehensive comprehension enables the creation of focused tactics that tackle every sector's distinct susceptibilities and adherence deficiencies, guaranteeing a solid safeguard against the ever-changing realm of cyber risks.

The suggested national cybersecurity framework, which prioritizes legislative obligations, collaborations between the public and commercial sectors, and strategic investments in cyberinfrastructure, presents a detailed plan for comprehensive national measures. This approach is crucial in establishing a robust cybersecurity ecosystem that safeguards Iraq's AIS against existing and new threats. Through promoting a culture that emphasises ongoing enhancement and careful monitoring, Iraq can effectively defend its essential infrastructures, maintain its position in the worldwide digital economy, and guarantee the security of sensitive data from unauthorised access.

The tables synthesize stakeholder viewpoints on AIS security, providing organisations with a means to assess their compliance level and a plan for further enhancement. By prioritising the suggested improvements, Iraqi organisations may effectively manage compliance intricacies, guaranteeing that their AIS (Automated Information Systems) maintains high security, durability, and reliability in response to ever-changing global standards and cyber risks. Adopting a proactive approach to compliance and cybersecurity is crucial in advancing Iraq's position in the global digital economy, promoting economic growth, and safeguarding data from unauthorised access.

The article highlights the importance of a comprehensive and well-planned strategy for cybersecurity in Iraq. The acquired insights emphasise the importance of resolving cybersecurity vulnerabilities and provide a roadmap for improving digital defenses. Implementing these suggested tactics and framework components will strengthen Iraq's cybersecurity position, safeguard its digital infrastructure, and support its economic stability and expansion. Pursuing a more secure digital future is intricate and ongoing, requiring collaborative endeavours from all parties involved, such as legislators, industry pioneers, and cybersecurity experts. By embracing these challenges and possibilities, Iraq may strive to protect itself against cyber dangers and flourish in the digital era, guaranteeing a safe and prosperous future for its population and enterprises.

References

[1] M. A. Kafi and N. Akter, (2023): Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. American Journal of Trade and Policy.
[2] C. Wang, W. Jiang, Y. Yu, H. Jing, Y. Qin and J. Li, (2023): Research on Information Security of Network Accounting Based on the Combination of Apriori and AOI Algorithms. 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT): 715-19.
[3] T. A. Abutaber, (2023): The impact of accounting information systems on enhancing financial information security in Jordanian banks. International Journal of Data and Network Science.
[4] J. McCallig, A. Robb and F. H. Rohde, (2019): Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. Int. J. Account. Inf. Syst., 33: 47-58.
[5] S. Lehenchuk, I. M. Vygivska and O. Hryhorevska, (2022): Protection of accounting information in the conditions of cyber security. Problems of Theory and Methodology of Accounting, Control and Analysis.
[6] J. Cai, (2023): Study on Data Security of Computerization under Centralized Accounting Mode. 2023 2nd International Conference on 3D Immersion, Interaction and Multi-sensory Experiences (ICDIIME): 342-46.
[7] F. Gu, (2023): Construction of an Accounting Information Security Management System Based on Artificial Intelligence Algorithms. 2023 2nd International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI): 42-46.

Journal of Ecohumanism
2024
Volume: 3, No: 5, pp. 293 – 315
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i5.3902

[8] O. Havryliuk, (2023): EFFECTIVE BUSINESS COMMUNICATION IN THE SYSTEM OF ACCOUNTING AND TAXATION. International scientific journal "Internauka". Series: "Economic Sciences".

[9] N. Jevtić and I. Alhudaidi, (2023): The importance of information security for organizations. Serbian Journal of Engineering Management.

[10] W. Zhou and M. Sun, (2022): Accounting Cyber Security Based on Blockchain. 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC): 1254-57.

[11] J. H. Kao and R. S. Tsay, (2023): Preventing Financial Statement Fraud with Blockchain-based Verifiable Accounting System. 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME): 1-5.

[12] B. L. a. Y. Jia, (2023): Design of Accounting Information System Based on Computer Network. International Journal of Multimedia Computing, 4(1): 121-30.

[13] M. I. Skrypnyk and O. Hryhorevska, (2020): ORGANIZATION OF ACCOUNTING INFORMATION PROTECTION IN TERMS OF CYBER SECURITY. Scientific Notes of Ostroh Academy National University, "Economics" Series.

[14] A. Susanto, (2018): Threats On Accounting Information Systems. International Journal of Scientific & Technology Research, 7: 51-53.

[15] B. Hu, (2021): Research on the Security of Accounting Information System in the Big Data Era. Academic Journal of Computing & Information Science.

[16] M. Neovius and B. Duncan, (2017): Anomaly Detection for Soft Security in Cloud based Auditing of Accounting Systems. International Conference on Cloud Computing and Services Science.

[17] L. Li, (2023): Data Security Technology in Electronic Commerce System Development. 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC): 1-6.

[18] S. W. J. Lin, W. N. Riccardi and C. Wang, (2019): Relative Effects of IFRS Adoption and IFRS Convergence on Financial Statement Comparability. Capital Markets: Market Efficiency eJournal.

[19] E. R. Kaburuan and A. S. L. Lindawati, (2019): Implementation of security system on humanitarian organization: case study of dompet dhuafa foundation. Journal of Physics: Conference Series, 1367(1): 012004.

[20] S. Bhagat and B. Bolton, (2013): Director Ownership, Governance, and Performance. Journal of Financial and Quantitative Analysis, 48(1): 105-35.

[21] I. M. Lopes, T. Guarda and P. Oliveira, (2020): General Data Protection Regulation in Health Clinics. Journal of Medical Systems, 44(2): 53.

[22] M. Wilnellys and F. Sarah, (2019): Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules. Journal of Nuclear Medicine Technology, 47(4): 269.

[23] R. M. B. Mohana, Anita & Ramamoorthy, Delshiw (2019): High Performance Network Intrusion Detection System. International Journal of Engineering and Advanced Technology, 9(2).

[24] C. C. Ngwakwe, (2022): Accounting Information System and Computerisation: A Conceptualisation. International Review of Management and Marketing, 12(2): 11-14.

[25] A. K. Ghazi-Tehrani and H. N. Pontell, (2021): Phishing Evolves: Analyzing the Enduring Cybercrime. Victims & Offenders, 16(3): 316-42.

[26] G. Mazzarolo and A. D. Jurcut, (2019): Insider threats in Cyber Security: The enemy within the gates. ArXiv, abs/1911.09575.

[27] A. Rhoda Iyanda and M. Ebenezer Fasasic, (2022): Development of Two-factor Authentication Login System Using Dynamic Password with SMS Verification. International Journal of Education and Management Engineering.

[28] E. Doynikova, A. Fedorchenko and I. Kotenko, (2019): Detection of Weaknesses in Information Systems for Automatic Selection of Security Actions. Automatic Control and Computer Sciences, 53: 1029 - 37.

[29] K. H. Shihan and M. J. Radif, (2022): Internal and External Factors to Adopt a Cyber Security Strategy in Iraqi Organisations. Webology.

[30] C. d. Montety, T. Antignac and C. Slim, (2019): GDPR Modelling for Log-Based Compliance Checking. IFIP International Conference on Trust Management.

[31] J. Seaman, (2020): PCI DSS Applicability.