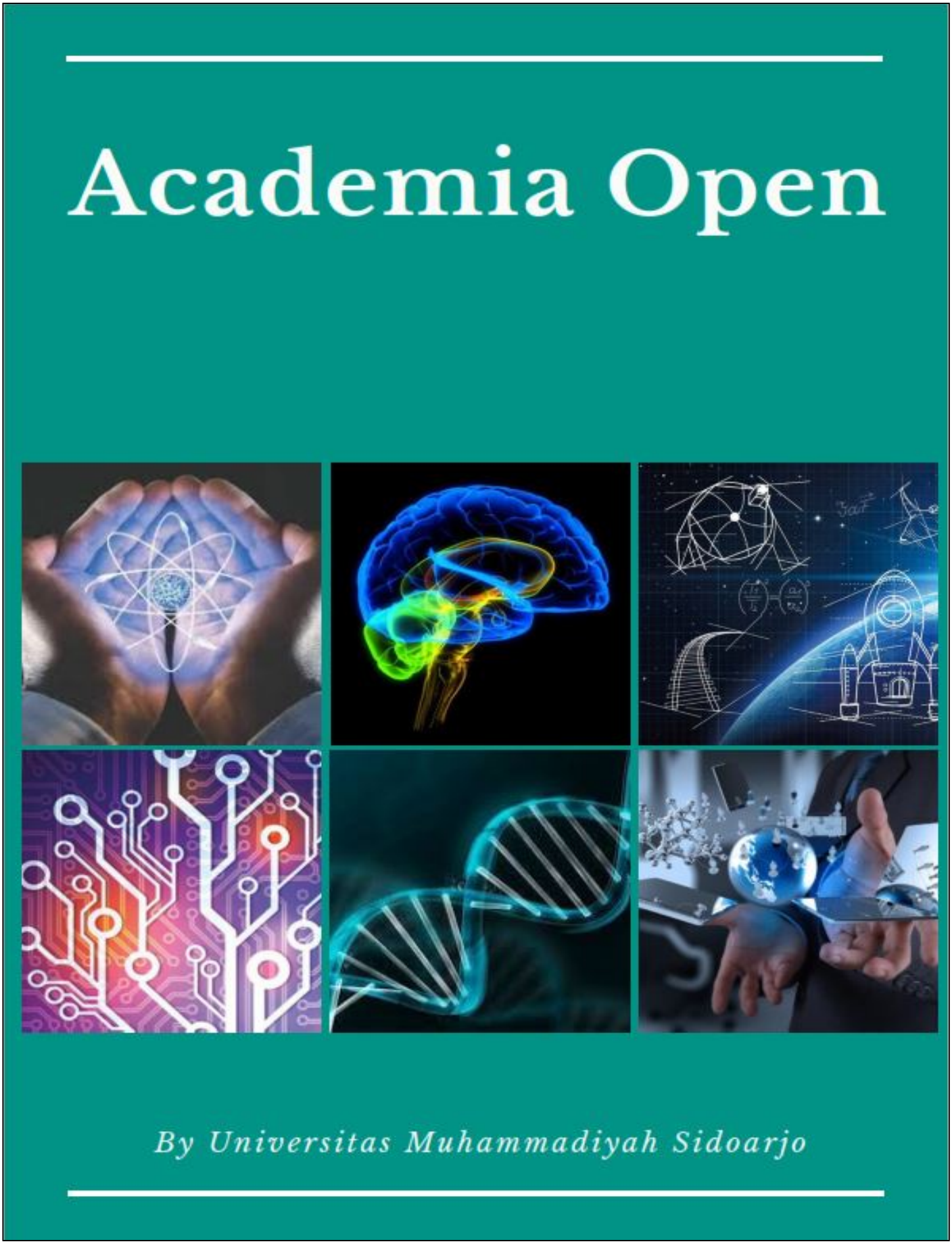
Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Table Of Content

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

EDITORIAL TEAM

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Cyber Attacks Undermine Audit Accuracy and Data Security in Banking

Serangan Siber Merusak Akurasi Audit dan Keamanan Data di Perbankan

Omar Mohammed Arkad, omar.mohammed@uoanbar.edu.iq, (1)
University of Anbar - Department of Administrative and Financial , Iraq

Adel Muwaffaq Kazim, adel89@uoanbar.edu.iq, (0)
University of Anbar - Department of Administrative and Financial , Iraq

Omar Ali Hadi, omar.ali@uoitc.edu.iq, (0)
UOITC - Department of Administrative and Financial , Iraq

(1) Corresponding author

Abstract

General Background: The rise of digital financial systems has increased banking institutions' exposure to cyber threats, particularly security system breaches, posing risks to data integrity and audit operations. **Specific Background:** Iraqi commercial banks have experienced frequent cyber attacks on accounting information systems, raising concerns about audit accuracy, data manipulation, and access delays. However, research on these threats' direct consequences for auditing remains scarce. **Knowledge Gap:** Prior studies emphasize cybersecurity measures but overlook how cyber attacks disrupt audit processes, transparency, and efficiency. **Aims:** This study evaluates security breaches' effects on auditing, assesses data manipulation risks, examines delays in financial access, and explores cyber incident investigations' role in mitigating threats. **Results:** Findings reveal that hacking compromises audit accuracy, causes operational delays, and threatens financial security, emphasizing the need for advanced cybersecurity measures. **Novelty:** This study bridges cybersecurity and auditing, providing empirical evidence on cyber threats' disruption of audit performance. **Implications:** Strengthening cybersecurity frameworks is essential for maintaining audit reliability and financial sector stability.

Highlights:

1. Cyber attacks compromise audit efficiency, data integrity, and financial security.
2. Hacking, data manipulation, and delays weaken audit accuracy and transparency.
3. Strengthening cybersecurity enhances audit reliability and banking sector stability.

Keywords: Cybersecurity, Audit, Cyberattacks, Accounting Information Systems

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Published date: 2025-05-01 13:58:40

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Introduction

As organizations increasingly rely on accounting information systems to manage financial operations and sensitive data, cyber security has become an integral part of protecting these systems. Cyber attacks pose an increasing threat to organizations around the world, including those that rely on accounting information systems in their daily operations. Auditing accounting information systems has become more complex in this digital age as auditors need to deal with cyber security risks as part of the audit process to ensure data integrity and audit efficiency. Auditing accounting information systems relies on the use of technology to ensure accuracy, transparency, and reliability in financial reporting. However, as technology evolves, new security challenges emerge, making organizations more vulnerable to cyber attacks. Cyber attacks are a major threat to audit efficiency, as they can cause system disruption, data corruption, or even unauthorized access to sensitive information. This research aims to study the role of cybersecurity in auditing accounting information systems, and how cyber attacks affect the efficiency and effectiveness of auditing operations

Methods

1.1. Research Problem: Iraqi banks suffer from an increase in cyber attacks that affect accounting information systems, which hinders the efficiency of auditing operations. The problem arises in how these attacks affect data protection, accuracy and speed of access, which may lead to increased costs and decreased audit quality. Therefore, it is necessary to understand the impact of these threats on auditing efficiency and determine appropriate methods to enhance them.

1.2. Research Hypothesis: The hypotheses of the current research are as follows:-

•Hypothesis 1: There is a statistically significant effect of the dimension of hacking security systems on auditing efficiency at a significance level of ($\alpha \leq 0.05$).

•Hypothesis 2: There is a statistically significant effect of the dimension of data manipulation on auditing efficiency at a significance level of ($\alpha \leq 0.05$).

•Hypothesis 3: There is a statistically significant effect of the dimension of delay in accessing data on auditing efficiency at a significance level of ($\alpha \leq 0.05$).

•Hypothesis 3: There is a statistically significant effect of the dimension of delay in accessing data on auditing efficiency at a significance level of ($\alpha \leq 0.05$).

•Hypothesis 4: There is a statistically significant effect of the cyber incident investigation dimension on audit efficiency at a significance level ($\alpha \leq 0.05$).

1.3. Research objectives: The current research aims to achieve the following:-

•Determine the extent of the impact of hacking security systems on the efficiency of auditing operations in Iraqi commercial banks.

•Analyze the impact of data manipulation resulting from cyber attacks on the accuracy and transparency of audit reports.

•Evaluate the impact of delays in accessing data on the speed and efficiency of completing audit procedures.

•Study the impact of cyber incident investigation on costs and adherence to the audit schedule.

1.4. Importance of the research

•The research contributes to providing a deep understanding of how cyber attacks affect the efficiency of auditing operations, which helps in developing more effective strategies to confront them.

•The research contributes to identifying security vulnerabilities in accounting information systems in banks, which enables improved protection and prevention procedures.

•The research provides evidence-based recommendations to improve auditing in light of cyber threats, which helps banks make informed decisions.

•By improving audit efficiency and reducing the impact of cyber attacks, the research contributes to enhancing the stability and security of the banking sector in Iraq.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

3.The concept of cybersecurity

Cybersecurity is the protection of systems, networks and programs from digital attacks that aim to access, change, destroy or disrupt sensitive information. Cybersecurity relies on a set of tools, techniques and procedures designed to secure information systems from external and internal threats. In the field of accounting, cybersecurity includes protecting accounting information systems and financial data from attacks that may result in loss or damage of data or theft of information [1].

Cybersecurity is also defined as a set of means, techniques and practices designed to protect systems, networks, programs and data from electronic attacks that target unauthorized access, destruction, modification or unauthorized disclosure [2].

Researchers believe that cybersecurity is defined as the practice of defending computers, servers, mobile phones, electronic systems, networks, and data from digital attacks, in order to ensure the confidentiality, integrity, and availability of information.

3.1. Accounting Information Systems and Cybersecurity

Accounting information systems are complex systems that rely on modern technology to facilitate the collection, processing, and storage of financial data. As reliance on these systems increases, so does the need to protect them from cyber threats. These threats may include unauthorized access, targeted attacks to sabotage data, or even financial manipulation carried out using malware. Cybersecurity in accounting information systems is essential to ensure the integrity and accuracy of financial information. In this context, security policies and procedures play a crucial role in protecting data from various threats. Institutions rely on technologies such as encryption, firewalls, and intrusion detection systems to ensure the security of accounting data [3].

Cyber threats have been a major challenge for banks since the 1990s. Banks in Iraq have worked to address this shift in cyber attacks by investing in security systems and leveraging the expertise needed to deal with information security. They have also been encouraged to adopt advanced systems that reduce potential risks. However, the level of penetration of these systems remains modest. Iraqi banks have a wide range of advanced electronic systems and IT assets that aim to enable them to access global markets as they rebuild their commercial presence. Iraqi commercial banks operate in a market full of security issues, and they consider the unstable regional environment to increase their level of risk [4]. These banks are significantly behind modern banks. The expansion in the availability of information technology has improved the ways in which banking operations are carried out, reduced operational costs and reliance on bank employees, and increased the customer base. However, the expanded use of technology has led to significant current, permanent, and future challenges, especially from a technical and security perspective. For example, Iraq has witnessed a number of low-intensity isolated attacks by hacking groups, along with denial-of-service attacks and ransomware attacks. In addition, there are ongoing and advanced cyber attacks aimed at influencing the political and military actions of other countries. The entire banking system and its users are at risk, as attackers and technical vulnerabilities do not distinguish between the public and banks [5].

Researchers believe that accounting information systems constitute a vital part of the financial infrastructure, as they rely heavily on technology to ensure the accuracy and speed of accounting operations. However, the reliance of these systems on modern technologies makes them vulnerable to cyber attacks, which requires advanced protection measures to ensure data integrity. Banks, especially in Iraq, face multiple challenges in this area, as they are exposed to cyber attacks aimed at hacking systems and disrupting operations. Therefore, it is necessary to improve the level of security in accounting information systems to keep pace with the increasing risks and ensure the effective protection of financial data.

3.2. Auditing practices in the banking sector

The supervisory work that has been developed specifically for the banking sector is subject to strict oversight due to strict regulatory requirements and the possibility of causing damage and losses that threaten the operational activities of banks. The accuracy and integrity of banking audits include fully protected operational mechanisms to prevent intrusion into customer confidentiality, as well as theft of electronic data and subsequent modification and economic losses resulting from the transactions executed. Management guidelines at the international level, related to the banking sector, and internal audit frameworks in force at the international level address multiple aspects, including those related to the banking sector. Internal audit practices are recognized as aiming to evaluate and improve risk management processes, control, governance processes, and the quality of information required to make sound decisions related to the strategic objectives of the banking entity. In addition to internal audit, external audit practices are also implemented in accordance with professional standards for auditing at the global level [6].

3.3.Cyber attacks: types and impact: Cyber attacks can take many forms, each of which can affect accounting information systems differently. Among the most common types of attacks are:

•Malware Attacks: Malware is malicious software designed to penetrate and damage systems. Malware can encrypt, delete, or even steal data, affecting the accuracy of financial information stored in accounting information

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

systems.

•Phishing Attacks: These attacks rely on tricking individuals into revealing sensitive information, such as passwords or login information to systems. If successful, attackers can access accounting information systems and manipulate or steal data [7].

•Denial of Service (DoS) attacks: These attacks aim to disrupt systems by loading them with huge amounts of illegitimate requests, causing the system to stop working. These attacks result in the inability to access or use accounting data, which greatly affects the efficiency of the audit.

•Insider Threats: Cyber threats may come from within the organization itself, whether intentionally or unintentionally. Unqualified or disgruntled employees can access accounting information systems and manipulate or leak data, posing a serious threat to cybersecurity [3].

3.4. The impact of cyber attacks on the audit of accounting information systems: Cyber attacks are a major threat to the audit of accounting information systems. When a hack or cyber attack occurs, the audit can be affected in several ways, including:

•Data loss: One of the biggest risks resulting from cyber attacks is the loss or corruption of financial data. If accounting information systems are attacked, auditors may lose access to the data necessary to conduct the audit, which affects the accuracy and reliability of the audit. Without accurate data, auditors cannot issue audit reports that reflect the true financial position of the organization.

•Data corruption and manipulation: In some cases, financial data may be manipulated as a result of cyber attacks. This manipulation may result in the issuance of inaccurate or misleading financial reports. Auditors must verify the validity of the data and verify whether it has been affected by any cyber attacks, which increases the complexity of the audit process [2].

•Disruption of systems: Cyberattacks that disrupt accounting information systems can significantly delay audits. If systems are unavailable to auditors, the audit process can be completely disrupted, delaying the preparation and submission of financial reports [3].

Several Iraqi commercial banks have been subjected to dozens of cyberattacks, especially at the electronic level, the most recent of which saw the targeting of ATMs of three banks in the fourth quarter of December 2018. Since cyberattacks are relatively recent events, the impact of cyber threats on operational efficiency has become a focus of attention for the management of all banks whose operations rely on cyber risks. Cyberattacks include unauthorized access, distributed denial of service attacks, and malware, which affect core banking systems. These security breaches are a priority for prevention. The direct and indirect effects of these attacks are usually characterized by financial losses and damage to reputation. The direct financial impact is the immediate monetary loss resulting from the criminal stealing a certain amount of money. Given the low level of protection against system intrusion and denial of service attacks, the indirect impact can also be considered; in fact, cyber attackers can disrupt and damage some of the computer systems used. The impact of these attacks is evident in the audit department of banks, as the efficiency of auditing operations is reduced due to the presence of security gaps in banking operations. Thus, the audit process is indirectly affected with banking operations by the occurrence of operational inefficiency [8]. The concepts of operational efficiency in this study refer not only to financial performance, but to the banking system as a whole. The non-financial aspect of the study results shows that the decline in efficiency is not only due to the national economy, but can also harm the general well-being of banks and stakeholders. This occurs through the time required to resolve the delay, which is negatively related to banking activity in general. Evaluating the impact of cyber attacks on efficiency shows that less costly banking requires a quick and effective response rather than ignoring it. The lack of banking services for bank customers is a common concern. If the operational side of banking operations is disrupted and banks are unable to operate efficiently, their ability to repay, receive loans, comply with regulations, and other economic recommendations is negatively affected. The data and expected conclusions from the study will increase the degree of business investment in effective cybersecurity strategies and products. The following study will focus on a different type of attacks and negative consequences on other potential benefits, losses in various assets of the banking system, or the financial operations of the community [9]. Researchers believe that cyber attacks pose significant challenges to the audit of accounting information systems, as they can lead to the loss or corruption of necessary data, which weakens the accuracy of financial reports. Data manipulation due to these attacks complicates the audit process, as it requires additional effort to ensure its accuracy. Disruption of systems increases the difficulties, as it may cause significant delays in auditing and reporting processes. Therefore, it is necessary to enhance cybersecurity to ensure the continuation of effective and reliable auditing.

3.5. The Role of Cybersecurity in Improving Audit Efficiency

Despite the threats posed by cyber attacks, cybersecurity can play an important role in improving the efficiency and effectiveness of auditing accounting information systems. By implementing strong security measures, the risks associated with cyber attacks can be reduced and the accuracy and transparency of financial reporting can be improved. Some of the security measures that can be applied include:

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

•Encryption and Data Protection: Encryption is a technique used to convert financial data into unreadable codes without a private key. By encrypting financial data in accounting information systems, organizations can protect their data from cyber threats. Encryption helps reduce the risk of data tampering or theft, ensuring the integrity of the information that auditors rely on for auditing [9]. Intrusion Detection Systems (IDS): Intrusion detection systems help monitor and respond to potential attacks before they cause significant damage. These systems can detect unusual activities or cyber threats in accounting information systems and alert the security team to take necessary action. This helps to reduce the impact of cyber attacks on the audit process.

•Security training and awareness: Awareness and training play an important role in enhancing cyber security within organizations. Employees should be trained on how to recognize cyber threats such as phishing emails and malware, and taught how to handle financial data securely. This reduces the likelihood of internal or unintentional attacks affecting accounting information systems [10].

•Backup systems: Backup systems allow organizations to restore financial data in the event of cyber attacks that result in data corruption or loss. These systems ensure the continuity of audit operations even if accounting information systems are compromised [3].

3.6. Cybersecurity response to reduce the impact of cyber attacks on accounting information systems audit

Addressing the impact of cyber attacks on accounting information systems audit requires organizations to take effective steps to ensure the continuity of accounting operations and prevent negative impacts on the audit. The cybersecurity response to these attacks can be summarized in several points:

•Implementing strict security policies: Establishing clear security policies and procedures is an essential step to reduce cyber risks. These policies include defining roles and access permissions to accounting information systems, establishing protocols to secure accounts, and applying strict rules regarding remote access. These policies can reduce the risk of unauthorized access to sensitive accounting data.

•Regular security audit: Auditing is not limited to financial systems only, but should also include periodic security audits. Cybersecurity audits help detect and correct vulnerabilities in the system before attackers can exploit them. This audit is essential to update and modify security policies to match new developments in cybersecurity threats [11].

•Access control techniques: Techniques such as two-factor authentication and identity and access management help in precisely controlling who can access accounting information systems. This enhances preventive measures and reduces the risk of internal and external threats [12].

•Compliance with international standards: Compliance with international security standards such as ISO/IEC 27001 helps organizations develop a comprehensive framework for managing security risks. Compliance with these standards enhances the confidence of auditors and stakeholders that the organization is taking adequate preventive steps to protect its accounting data [13].

With the increase in cyber threats, electronic governance has become an integral part of the security strategies of organizations that rely on accounting information systems. Electronic governance refers to the policies and organizational structures that are put in place to ensure that information technology is used safely and in an organized manner in the organization.

•Promoting electronic governance for information safety: Electronic governance plays a crucial role in ensuring that accounting information systems are used in accordance with defined security policies and procedures. This includes defining individuals’ responsibilities towards cyber security and establishing protocols for responding to potential cyber threats. E-governance helps reduce the likelihood of cyber attacks and increases the organization's ability to respond quickly and efficiently.

•Security Risk Management under E-governance: E-governance helps in continuously assessing security risks and updating preventive measures based on the analysis of these risks. Through effective security risk management, the organization can protect its financial data and maintain the continuity of accounting operations even in the event of attacks [14].

Researchers believe that confronting the impact of cyber attacks on the audit of accounting information systems requires the adoption of strong preventive measures that include strict security policies and continuous auditing of systems. Access control technologies such as two-factor authentication help reduce the risks related to unauthorized access. Adherence to international standards enhances data protection and increases the reliability of accounting systems. E-governance plays an important role in regulating the use of technology, which supports effective risk management and ensures the continuity of accounting operations even in emergency situations.

3.7. Future Challenges and Emerging Trends: Despite efforts to improve cybersecurity in auditing accounting information systems, challenges still exist. The most prominent of these challenges are: [15]

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

•Adapting to new and changing threats: Cyber threats are constantly evolving, requiring organizations and auditors to stay aware of new trends in attacks. Complex attacks such as AI-based attacks and those targeting cloud infrastructure pose a major challenge to the field of cybersecurity. This requires rapid adaptation to new threats and updating preventive measures.

•Lack of security skills: One of the biggest challenges facing organizations is the shortage of specialized competencies in the field of cybersecurity. Training auditors to use modern technologies to detect and analyze threats is an additional challenge. Therefore, organizations must focus on developing human capabilities alongside technological developments.

Cybersecurity is an imperative to ensure the safety of accounting information systems in light of increasing cyber threats. Security policies and technical measures play a vital role in protecting accounting data and ensuring the continuity of auditing operations. Through cooperation between audit and cybersecurity teams, effective protection of accounting information systems can be achieved and the risk of attacks can be reduced. Despite the challenges facing organizations in this area, progress in the field of electronic governance, risk management, and the development of security skills can enhance audit efficiency and ensure the integrity of financial operations.

Researchers believe that despite efforts to improve cybersecurity in auditing accounting information systems, challenges remain. The continuous development of threats, such as attacks based on artificial intelligence and cloud infrastructure, requires organizations to adapt quickly. The lack of security skills is a major challenge, which calls for the development of human capabilities alongside modern technologies. Cooperation between audit and cybersecurity teams can enhance protection and ensure audit efficiency, which helps address threats and achieve continuity of accounting operations.

4. The practical aspect

In this study, a research methodology was adopted that combines theoretical and applied aspects, with the aim of understanding the role of cybersecurity in auditing accounting information systems and the impact of cyber attacks on audit efficiency in Iraqi commercial banks. The study targets accounting and auditing employees at Al-Rasheed and Middle East Banks in Baghdad, where 135 questionnaires were distributed, and 127 of them were analyzed. The questionnaire was used as a tool to measure the impact of cyber attacks on the efficiency of auditing accounting information systems. The data were analyzed using SPSS through descriptive statistics, variance analysis, and regression. The results showed the impact of attacks on auditing efficiency, identifying the most influential dimensions. The study focused on cybersecurity strategies to enhance auditing efficiency in Iraqi commercial banks. I. Validity of the questionnaire tool

In this study, the validity of the questionnaire tool was verified to ensure its accurate measurement of the impact of cyber attacks on the efficiency of auditing accounting information systems. This was done through face validity, which shows the clarity and validity of the questions asked, which is essential for the success of the study. The questionnaire was submitted to five arbitrators specialized in the field of accounting to evaluate it and verify its suitability and accuracy. The arbitrators focused on whether the questions clearly reflect the study variables and aim to measure concepts related to cybersecurity and auditing efficiency. Based on the reviewers' comments, some modifications were made to enhance the clarity of the questions and their consistency with the research objectives.

To assess the reliability of the questionnaire, Cronbach's alpha coefficient was calculated, which is used to determine the degree of internal consistency of the statements within each dimension of the questionnaire. Cronbach's alpha coefficient indicates the degree of consistency between the questions related to each dimension, where the acceptable value is usually 0.70 or higher. In this study, the questionnaire achieved a good level of Cronbach's alpha coefficient, indicating that the tool used has a high degree of reliability and validity, which enhances the reliability of the results extracted from the collected data.

Variable	NO.	Cronbach's alpha coefficient
After security breach	5	.805
After data manipulation	5	.830
After delay in accessing data	5	.798
After cyber incident investigation	5	.868
Audit efficiency (dependent variable)	8	.817

Table 1. *Cronbach's alpha coefficient for the study variables*

4.1.Demographic data

%	NO.	Items
73.2	93	Male
26.8	34	Female

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

100.0	127	Total

Table 2. *Research sample by gender*

It is noted in Table (2) that the number of males in the sample is 93, representing 73.2% of the total sample, which is the largest percentage. As for the number of females, it is 34, representing 26.8% of the total sample.

%	NO.	Items
12.6	16	20-30 years
22.8	29	30 -40 years
37.0	47	40-50 years
27.6	35	50 years
100.0	127	Total

Table 3. *Research sample according to age*

The table shows that the majority of the study participants are from the age group of more than 40-50 years at 37%, followed by the age group of 50 years and above at 27.6%, indicating that most of the sample has long experience in accounting and auditing. While the age group of more than 30-40 years constitutes 22.8%, and the age group of 20-30 years represents only 12.6%. This distribution reflects that the sample consists mainly of experienced people, which enhances the reliability of the research results.

%	NO.	Items
7.9	10	Preparatory
8.7	11	Technical Diploma
61.4	78	Bachelor's
7.9	10	Higher Diploma
3.9	5	Master's
4.7	6	PhD
5.5	7	Chartered Accountant
100.0	127	Total

Table 4. *Research sample according to academic qualification*

Table (4) shows the distribution of the research sample according to the academic qualifications of the participants. We note that bachelor's degree holders constitute the largest percentage of the sample at 61.4% (78 participants), which reflects that most of those working in auditing and accounting within banks have a bachelor's degree as a minimum. The other categories were distributed as follows: preparatory and higher diploma at 7.9% each (10 participants), and technical diploma at 8.7% (11 participants), which indicates that there is a percentage of workers who have intermediate or specialized qualifications.

As for the higher educated categories, such as master's and doctorate, their percentage was low, reaching 3.9% for master's (5 participants) and 4.7% for doctorate (6 participants). This indicates that a small number of workers in this field have higher academic degrees. The last category is chartered accountants, who constitute 5.5% (7 participants), which reflects the presence of a small specialized category with advanced professional qualifications in accounting.

%	NO.	Items
10.2	13	Less than 5 years
16.5	21	5-10 years
48.0	61	10-15 years
25.2	32	More than 15 years
100.0	127	Total

Table 5. *Research sample according to years of experience*

The sample shows that the majority of participants have experience ranging from 10 to 15 years at 48%, reflecting an average level of experience. This is followed by the category of more than 15 years at 25.2%, indicating a large number of people with deep experience. The category of 5 to 10 years constitutes 16.5%, while the category of less than 5 years is the least at 10.2%. This distribution reflects the diversity of experience, which supports their assessments of the impact of cybersecurity on auditing.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

%	NO.	Items
50.4	64	Accounting
15.0	19	Management
15.7	20	Economics
8.7	11	Financial Sciences
10.2	13	Other
100.0	127	Total

Table 6. *Research sample by type of qualification*

The sample shows that 50.4% of the participants hold qualifications in accounting, reflecting the main specialization in the study. The remaining percentage is distributed between management specializations (15%) and economics (15.7%), with a smaller representation of financial sciences (8.7%). The other category includes 10.2% of the sample, indicating a diversity of scientific backgrounds. This diversity enhances the understanding of the impact of cybersecurity on the efficiency of accounting auditing.

Result and Discussion

•After hacking security systems

Table (7) displays the arithmetic means, standard deviations, order and level of importance for the first dimension (after hacking security systems) for the independent variable (cyber attacks) as follows:-

Importance	Rank	Stand. Dev.	mean	Expressions
High	1	.690	4.27	Security breaches lead to weaker financial data protection
Good	3	.873	4.13	Security breaches make it difficult to access information needed for the audit process
High	2	.758	4.25	You see auditors facing greater challenges when dealing with security breaches during audits
Good	5	.855	3.85	Security breaches affect the reliability of the financial data being audited
Good	4	.937	4.06	Dealing with security breaches requires longer time to complete the audit process
Good		.612	4.110	Total

Table 7. *Arithmetic means and standard deviations for the dimension of hacking security systems*

The table shows the results of the statistical analysis of the dimension (security systems penetration), which is one of the dimensions of the independent variable (cyber attacks):-

-The highest-rated statement was: "Security systems penetration leads to weak protection of financial data", with an arithmetic mean of 4.27 and a standard deviation of 0.690, reflecting a high level of importance.

-The statement came in second place: "Auditors believe that they face greater challenges when dealing with security systems penetration during audits", with an arithmetic mean of 4.25 and a standard deviation of 0.758, also indicating a high level of importance.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

-As for the other statements, their levels ranged between good and high, with arithmetic means ranging between 3.85 and 4.13, reflecting a clear impact of systems penetration on audit efficiency, with different degrees of importance for the statements.

-In general, the table indicates that the penetration of security systems has a significant impact on the protection of financial data, ease of access to information, data reliability, and audit time, which reflects a significant impact on accounting audits in banks.

•Data manipulation dimension

Table (8) shows the arithmetic means, standard deviations, ranking, and level of importance for the second dimension (data manipulation dimension) for the independent variable (cyber attacks) as follows:-

Importance	Rank	Stand. Dev.	mean	Expressions
good	2	.876	4.13	Cyber attacks are a major cause of financial data manipulation within an organization
good	1	.740	4.31	Data manipulation reduces the accuracy of final audit reports
good	5	.858	4.04	Auditors find it difficult to detect data manipulation resulting from cyber attacks
good	4	.771	4.04	Data manipulation affects the transparency and objectivity of the audit process
good	3	.702	4.09	You see that data manipulation due to cyber attacks increases the efforts spent on conducting the audit process
good		.612	4.111	Total

Table 8. *Arithmetic means and standard deviations for the data manipulation dimension*

-The table shows the results of the statistical analysis of the dimension (data manipulation). The statement: "Data manipulation reduces the accuracy of final audit reports" received the highest arithmetic mean of 4.31 and a standard deviation of 0.740, indicating that participants consider it the most important in this dimension. It is followed by the statement: "Cyber attacks are a major cause of financial data manipulation within the organization" with an arithmetic mean of 4.13 and a standard deviation of 0.876, reflecting a good awareness of the impact of attacks on data.

-The other statements recorded close arithmetic means ranging between 4.04 and 4.09, reflecting the clear impact of cyber attacks on the difficulty of detecting manipulation, reducing audit transparency, and increasing the efforts made.

In general, the table shows that data manipulation as a result of cyber attacks has a noticeable impact on the accuracy of audit reports, process transparency, and increasing the efforts made, highlighting the role of cybersecurity in improving audit efficiency and reducing the impact of manipulation.

•After the delay in accessing data

Table (9) shows the arithmetic means, standard deviations, order and level of importance for the third dimension (after the delay in accessing data) for the independent variable (cyber attacks) as follows:-

Importance	Rank	Stand. Dev.	mean	Expressions
good	4	.85692	3.9504	Cyber attacks delay auditors' access to

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

				financial data
good	1	1.01368	4.1764	Delays in accessing data cause difficulties in performing audit procedures on time
good	3	.89073	3.9843	Delays in accessing data lead to lower quality of audit reports
good	2	.89974	4.0000	Cyber attacks affect the ease and speed of obtaining supporting evidence for the audit process
good	5	.96742	3.8661	Delays in accessing data as a result of cyber attacks are an obstacle to completing audits efficiently
good		.618	3.981	Total

Table 9. *Arithmetic means and standard deviations for the dimension of the delay in accessing data*

The table shows the results of the statistical analysis of the dimension of delay in accessing data, which is one of the dimensions of the independent variable (cyber attacks):-

-The statement: “Delay in accessing data causes difficulties in implementing audit procedures on time” obtained the highest arithmetic mean of 4.18 and a standard deviation of 1.01, reflecting its high importance in influencing audit efficiency.

-It is followed by the statement: “Cyber attacks affect the ease and speed of obtaining evidence supporting the audit process” with an arithmetic mean of 4.00 and a standard deviation of 0.89, indicating that participants see a significant impact of attacks on the effectiveness of accessing evidence.

-The statement: “Delay in accessing data leads to a decrease in the quality of audit reports” recorded an arithmetic mean of 3.98, indicating a tangible impact of attacks on the quality of final reports. The statement with the lowest rating was: “Delays in accessing data as a result of cyber attacks are an obstacle to completing audits efficiently”, with an arithmetic mean of 3.87, but it still shows a clear impact on the efficiency of Audit.

The table indicates that the delay in accessing data resulting from cyber attacks is a factor affecting the implementation of audit procedures, the speed of obtaining evidence, and the quality of final reports, which highlights the importance of enhancing cyber security to ensure audit efficiency.

•After investigating cyber incidents

Table (10) displays the arithmetic means, standard deviations, ranking, and level of importance for the fourth dimension (after investigating cyber incidents) for the independent variable (cyber attacks) as follows:-

Importance	Rank	Stand. Dev.	mean	Expressions
High	1	.67745	4.2205	Auditors spend a lot of time investigating cyber incidents
High	2	.78010	4.2047	Cyber incidents add complexity to the audit process
Good	4	.78989	4.0551	Cyber incident investigations provide more accurate data for the audit process
Good	5	.97776	3.8898	Cyber incident investigations impact adherence to audit timelines
Good	3	.73489	4.0866	Cyber investigations

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

				add additional burden to the audit process
Good		.645	4.091	Total

Table 10. *Arithmetic means and standard deviations for the dimension of investigating cyber incidents*

The table shows the results of the statistical analysis of the dimension of investigating cyber incidents, which is one of the dimensions of the independent variable (cyber attacks):-

-The statement: "Auditors take a long time to investigate cyber incidents" came in first place with an arithmetic mean of 4.22 and a standard deviation of 0.68, indicating that participants see it as the most influential in this dimension, with a high level of importance. It was followed by the statement: "Cyber incidents increase the complexity of the audit process" with an arithmetic mean of 4.20 and a standard deviation of 0.78, indicating a noticeable impact of cyber incidents on the complexity of the audit.

-The statement: "Cyber investigations constitute an additional burden on the audit process" also recorded an arithmetic mean of 4.09, reflecting a clear impact of investigations on audit processes. The statement with the lowest rating was: "Investigating cyber incidents affects adherence to audit timelines", with an arithmetic mean of 3.89, but it still indicates a noticeable negative impact on adherence to deadlines.

The table indicates that cyber incident investigation is a factor affecting the duration of the audit, its complexity, and adherence to timelines, which highlights the importance of managing cyber incidents effectively to ensure the efficiency of the audit process.

•Audit Efficiency

Table (11) shows the arithmetic means, standard deviations, ranking, and level of importance of the dependent variable audit efficiency as follows:-

Importance	Rank	Stand. Dev.	mean	Expressions
Good	5	.926	4.092	The efficiency of the audit process is negatively affected when systems are exposed to cyber attacks
Good	7	.816	3.981	Cyber attacks reduce the ability of auditors to perform their tasks effectively
Good	3	.767	4.15	You find that auditors are able to overcome the challenges posed by cyber attacks during the audit process
High	1	.709	4.31	Cyber attacks affect the accuracy of audit results
Good	4	.735	4.095	You consider that efforts made to improve audit efficiency are sufficient to deal with cyber threats
Good	6	.919	4.071	Digital auditing can improve the efficiency of the audit process in the face of cyber threats
Good	2	.761	4.27	Cyber attacks lead to increased audit costs
Good	8	.843	3.81	Additional protection measures affect audit efficiency in the face

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

				of cyber attacks
Good		.538	4.096	Total

Table 11. *Arithmetic means and standard deviations of audit efficiency*

The table shows the results of the statistical analysis of the dependent variable (audit efficiency) and the impact of cyber attacks on it, as follows: -

-The statement: "Cyber attacks affect the accuracy of audit results" came in first place with an arithmetic mean of 4.31 and a standard deviation of 0.709, reflecting a high awareness of the impact of attacks on the accuracy of the final results. It was followed by the statement: "Cyber attacks lead to increased audit costs" with an arithmetic mean of 4.27, indicating the importance of costs as a factor affecting audit efficiency. Also, the statement: "Auditors are able to overcome the challenges imposed by cyber attacks" achieved an arithmetic mean of 4.15, reflecting a good level of adaptation to challenges.

-As for the statement: "The efficiency of the audit process is negatively affected when systems are exposed to cyber attacks", it recorded an arithmetic mean of 4.09, indicating the impact of attacks on audit efficiency. The least rated statement was: "Additional protection measures affect audit efficiency" with an arithmetic mean of 3.81, but it still reflects a clear impact on audit efficiency in the face of cyber attacks.

-The table indicates that cyber attacks significantly affect the accuracy of audit results, its costs, and the ability of auditors to adapt to challenges, which highlights the need to enhance preventive measures and improve audit efficiency to confront cyber threats.

5.3. Hypothesis Testing

•Hypothesis Testing: There is a statistically significant impact of the security systems penetration dimension on audit efficiency at a significance level (α ≤ 0.05).

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	R	R2
		B	Std. Error	Beta				
1	(Constant)	1.109	.183		6.046	.000	827a	685
	□□□□□□ □□□□□□ □□□□□□	.727	.044	.827	16.469	.000		
a. Dependent Variable: Audit efficiency (dependent variable)								

Table 12. *The impact of security systems penetration on audit efficiency*

a. Dependent Variable: Audit efficiency (dependent variable)

The table shows the results of the first hypothesis test, which assumes that there is a statistically significant effect of the security systems penetration dimension on audit efficiency at a significance level (α ≤ 0.05).

-The unstandardized regression coefficient (B) for the security systems penetration dimension is 0.727, which means that there is a positive effect of each unit increase in systems penetration on audit efficiency. The standardized Beta value is 0.827, which indicates the strength of the relationship between systems penetration and audit efficiency.

-The calculated t value was **16.469, which is statistically significant at the Sig. = 0.000** level, which means that the effect is significant and with a large difference.

-The R value is estimated at 0.827, which indicates a strong association between systems penetration and audit efficiency. The R^2 value (0.685) indicates that about 68.5% of the change in audit efficiency can be explained by the effect of security systems penetration, which highlights the importance of this dimension in influencing the efficiency of audit operations.

The results indicate that there is a clear statistical impact of hacking security systems on audit efficiency, which confirms the validity of the first hypothesis and calls for adopting security protection enhancement measures to contribute to raising audit efficiency in banks.

•Testing the second hypothesis: There is a statistically significant impact of the data manipulation dimension on audit efficiency at a significance level of (α ≤ 0.05).

Academia Open
Vol 10 No 1 (2025): June (In Progress)
DOI: 10.21070/acopen.10.2025.10686 . Article type: (Computer Science)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	R	R2
		B	Std. Error	Beta				
1	(Constant)	1.166	.191		6.103	.000	811a	661
	□□□□□□ □□□□□□□□□	.713	.046	.811	15.514	.000		
a. Dependent Variable: Audit efficiency (dependent variable)								

Table 13. *The impact of data manipulation on audit efficiency*

a. Dependent Variable: Audit efficiency (dependent variable)

The table shows the results of the second hypothesis test, which assumes that there is a statistically significant effect of the data manipulation dimension on audit efficiency at a significance level (α ≤ 0.05).

-The unstandardized regression coefficient (B) for the data manipulation dimension is 0.713, indicating a positive effect, as each increase in data manipulation leads to a negative effect on audit efficiency. The standardized Beta value is 0.811, reflecting a strong relationship between data manipulation and audit efficiency.

-The calculated t value is 15.514, which is statistically significant at the Sig. = 0.000** level, meaning that the effect of data manipulation on audit efficiency is significant.

-The R value is estimated at 0.811, indicating a strong relationship between data manipulation and audit efficiency. The R^2 value (0.661) indicates that about 66.1% of the change in audit efficiency can be explained by the effect of data manipulation, which highlights the importance of this dimension in influencing audit processes.

The results confirm that data manipulation has a clear statistical effect on audit efficiency, which supports the second hypothesis, and indicates the need to develop more stringent audit mechanisms to detect manipulation and maintain the accuracy and effectiveness of audit processes.

•Testing the third hypothesis: There is a statistically significant effect of the dimension of delay in accessing data on audit efficiency at a significance level (α ≤ 0.05).

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	R	R2
		B	Std. Error	Beta				
1	(Constant)	1.764	.188		9.402	.000	742a	581
	□□ □□□□□□□ □□□ □□□□□□ □□□□□□□□	.593	.047	.748	12.615	.000		
a. Dependent Variable: Audit efficiency (dependent variable)								

Table 14. *The effect of delay in accessing data on audit efficiency*

a. Dependent Variable: Audit efficiency (dependent variable)

The table shows the results of the third hypothesis test, which assumes that there is a statistically significant effect of the delay in accessing data on audit efficiency at a significance level (α ≤ 0.05).

-The unstandardized regression coefficient (B) for the delay in accessing data is 0.593, indicating a negative effect, as delay in accessing data leads to a decrease in audit efficiency. The standardized Beta value is 0.748, reflecting a strong relationship between delay in accessing data and audit efficiency.

-The calculated t value is 12.615, which is statistically significant at the Sig. = 0.000** level, indicating that the effect of delay in accessing data on audit efficiency is significant.

-The R value is estimated at 0.742, indicating a strong association between delay in accessing data and audit efficiency. The R^2 value (0.581) indicates that about 58.1% of the change in audit efficiency can be explained by the effect of the delay in accessing data, which highlights the importance of this dimension in influencing auditing processes.

The results confirm the existence of a clear statistical effect of the delay in accessing data on auditing efficiency, which supports the third hypothesis and indicates the need to improve the speed of data access to avoid negative

effects on auditing processes.

iv. Testing the results of the fourth hypothesis: There is a statistically significant effect of the cyber incident investigation dimension on auditing efficiency at a significance level (α ≤ 0.05).

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	R	R2
		B	Std. Error	Beta				
1	(Constant)	1.131	.152		7.430	.000	870a	761
	□□ □□□□□□□ □□□□□□□ □□□□□□□□□□	.725	.037	.870	19.718	.000		
a. Dependent Variable :Audit efficiency (dependent variable)								

Table 15. *The effect of cyber incident investigation on auditing efficiency*

a. Dependent Variable :Audit efficiency (dependent variable)

The table shows the results of the fourth hypothesis test, which assumes a statistically significant effect of the cyber incident investigation dimension on audit efficiency at a significance level (α ≤ 0.05).

-The unstandardized regression coefficient (B) for the cyber incident investigation dimension is 0.725, indicating a positive effect, as cyber incident investigation leads to enhancing audit efficiency. The standardized Beta value is 0.870, reflecting a very strong relationship between cyber incident investigation and audit efficiency.

-The calculated t value is 19.718, which is statistically significant at the Sig. = 0.000** level, confirming that the effect of cyber incident investigation on audit efficiency is significant.

-The R value is estimated at 0.870, indicating a very strong relationship between cyber incident investigation and audit efficiency. The R^2 value (0.761) indicates that about 76.1% of the change in audit efficiency can be explained by the impact of cyber incident investigation, which highlights the role of this dimension in improving audit operations.

The results confirm the existence of a strong and clear statistical impact of cyber incident investigation on audit efficiency, which supports the fourth hypothesis and indicates the importance of improving investigation techniques and procedures to enhance audit efficiency in banks.

Conclusion

•The results demonstrate the importance of developing advanced tools and techniques for investigating cyber incidents, which will practically contribute to improving the efficiency of audit operations in Iraqi banks by effectively confronting cyber attacks and mitigating their effects.

•Hacking security systems significantly affects audit efficiency, as it exposes financial data to risk, which necessitates the activation of protection protocols to reduce the risks of these hacks.

•Data manipulation resulting from cyber attacks negatively affects the quality and transparency of audit reports, indicating that auditing requires more efficient systems to detect and address manipulation quickly.

•Delays in accessing data lead to a decline in audit efficiency, which reflects the need to improve access to protected financial data to achieve greater effectiveness in audit operations.

•Investigating cyber incidents plays a fundamental role in improving audit efficiency, as it enhances the accuracy and effectiveness of audit operations, which highlights the need to adopt advanced technologies to detect and analyze incidents effectively.

References

1. M. G. Alles and G. L. Gray, "The Role of Big Data in Fraud Detection: A Survey of Financial Statement Auditors," J. Account. Lit., vol. 36, pp. 27-46, 2016.
2. R. Anderson and T. Moore, "The Economics of Information Security," Science, vol. 314, no. 5799, pp. 610-613, 2007.
3. M. Bishop, Computer Security: Art and Science, 2nd ed. Boston, MA, USA: Addison-Wesley, 2018.

4. A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th ed. London, U.K.: Kogan Page, 2024.
5. P. H. Gregory, CISSP Guide to Security Essentials, New York, NY, USA: McGraw-Hill Education, 2015.
6. A. Hovav and J. D'Arcy, "Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea," Inf. Manage., vol. 49, no. 2, pp. 99-110, 2012.
7. M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of Security Threats in Information Systems," Procedia Comput. Sci., vol. 32, pp. 489-496, 2014.
8. A. Kaplan and M. Haenlein, "Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence," Bus. Horiz., vol. 62, no. 1, pp. 15-25, 2019.
9. W. F. Messier, S. M. Glover, and D. F. Prawitt, Auditing and Assurance Services: A Systematic Approach, 11th ed. New York, NY, USA: McGraw-Hill Education, 2019.
10. S. Posthumus and R. von Solms, "A Framework for the Governance of Information Security," Comput. Secur., vol. 23, no. 8, pp. 638-646, 2004.
11. M. B. Romney and P. J. Steinbart, Accounting Information Systems, 15th ed. Boston, MA, USA: Pearson, 2020.
12. P. Weill and J. W. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Boston, MA, USA: Harvard Business School Press, 2004.
13. S. A. Zbar, "Requirements to Support a Management Information System to Confront the Cyber Threat in the Iraqi Trade Bank," Russ. Law J., vol. 11, no. 3, pp. 736-759, 2023.
14. K. H. Shihan and M. J. Radif, "Internal and External Factors to Adopt a Cyber Security Strategy in Iraqi Organisations," Webology, vol. 19, no. 1, pp. 5181-5198, 2022.
15. I. A. Hamidi and K. S. Hussein, "The Impact of Cyber Risk Management on the Strategy for Protecting Financial Assets: Descriptive and Analytical Research of the Opinions of a Sample of Employees in the Trade Bank of Iraq," Conf. Lit. Humanit. Nat. Sci., 2024.
16. M. F. Hasan and N. S. Al-Ramadan, "Cyber-Attacks and Cyber Security Readiness: Iraqi Private Banks Case," Soc. Sci. Humanit. J. (SSHJ), pp. 2312-2323, 2021.
17. P. Rikhardsson, C. Rohde, L. Christensen, and C. E. Batt, "Management Controls and Crisis: Evidence from the Banking Sector," Account. Audit. Accountab. J., vol. 34, no. 4, pp. 757-785, 2021.
18. K. A. McEwan, "Cyber-Threats as Political Risk: Increased Risk for the Oil and Gas Industry," Ph.D. dissertation, Stellenbosch Univ., Stellenbosch, South Africa, 2020.
19. M. A. Saada and Y. Turan, "Intelligent System for Measurement and Appreciate a Country Power, Capabilities," J. Inf. Sci. Eng., vol. 37, no. 6, 2021.
20. A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 5th ed. London, U.K.: Kogan Page, 2015.
21. W. N. Wan-Hussin, H. Fitri, and B. Salim, "Audit Committee Chair Overlap, Chair Expertise, and Internal Auditing Practices: Evidence from Malaysia," J. Int. Account. Audit. Taxation, vol. 44, p. 100413, 2021.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo