Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

The relationship between adopting cloud computing technologies to enhance the cybersecurity of accounting information systems and its impact on corporate sustainability

Sarah Alawi Maryoush*[A], Ilham Mohammed Wathiq Al-Obaidi [A], Muna Kamel Hamad [B]

[A] College of Administration and Economics/Iraqi University
[B] College of Administration and Economics/NahRaiaN University

Keywords:
Cloud computing technologies, cybersecurity, accounting information systems, corporate sustainability.

Article history:
Received 16 Jan. 2025
Accepted 23 Jan. 2025
Available online 25 Jun. 2025

*Corresponding author:
Sarah Alawi Maryoush
College of Administration and Economics/Iraqi University

Abstract: The rapid evolution of digital technology has introduced unprecedented cybersecurity threats, affecting corporate sustainability. Organizations increasingly rely on IT, AI, and electronic accounting systems, exposing them to significant risks. This study explores how cloud computing enhances the cybersecurity of accounting information systems and supports corporate sustainability.

A combined deductive and inductive approach was employed. Theoretical aspects were analyzed using references from Arabic and foreign sources, while practical aspects focused on cloud computing technologies, cybersecurity risks, and mitigation strategies. The study examined the case of Zain Iraq Telecommunications, which suffered a cyberattack in 2022, leading to the theft of 26 million dinars from customer wallets.

Cybersecurity was evaluated using the Global Cybersecurity Index (GCI) to assess the company's commitment to protecting its accounting information systems. Risk analysis was conducted using SWOT for strengths, weaknesses, opportunities, and threats, while OCTAVE assessed accounting information system vulnerabilities. Cyber risk measurement combined quantitative analysis using FAIR and qualitative assessment through the Risk Matrix.

To determine the financial impact of the cyberattack, Tobin's Q was applied to measure the company's value before and after the security breach. The findings revealed that Zain Iraq did not disclose the cybersecurity incident in its annual report, despite the substantial financial losses incurred. This underscores the need for transparency and stronger cybersecurity measures to ensure corporate resilience in the digital age.

العلاقة بين تبني تقنيات الحوسبة السحابية لتعزيز الأمن السيبراني لأنظمة المعلومات المحاسبية وتأثيرها على استدامة الشركات

سارة العلوي مريوش
كلية الإدارة والاقتصاد
الجامعة العراقية

الهام محمد واثق العبيدي
كلية الإدارة والاقتصاد
الجامعة العراقية

منى كامل حمد
كلية الإدارة والاقتصاد
جامعة النهرين

المستخلص

أدى التطور السريع للتكنولوجيا الرقمية إلى ظهور تهديدات غير مسبوقة للأمن السيبراني، مما أثر على استدامة الشركات. تعتمد المؤسسات بشكل متزايد على تكنولوجيا المعلومات والذكاء الاصطناعي وأنظمة المحاسبة الإلكترونية، مما يعرضها لمخاطر كبيرة. تستكشف هذه الدراسة كيف تعزز الحوسبة السحابية الأمن السيبراني لأنظمة المعلومات المحاسبية وتدعم استدامة الشركات.

تم استخدام نهج استنتاجي واستقرائي مشترك. تم تحليل الجوانب النظرية باستخدام مراجع من مصادر عربية وأجنبية، بينما ركزت الجوانب العملية على تقنيات الحوسبة السحابية ومخاطر الأمن السيبراني واستراتيجيات التخفيف. تناولت الدراسة حالة شركة زين العراق للاتصالات، التي تعرضت لهجوم إلكتروني في عام 2022، مما أدى إلى سرقة 26 مليون دينار من محافظ العملاء. تم تقييم الأمن السيبراني باستخدام مؤشر الأمن السيبراني العالمي (GCIلتقييم التزام الشركة بحماية أنظمة المعلومات المحاسبية الخاصة بها. تم إجراء تحليل المخاطر باستخدام تحليل SWOT لنقاط القوة والضعف والفرص والتهديدات، بينما قام تحليل OCTAVE بتقييم نقاط ضعف نظام المعلومات المحاسبية. جمع قياس المخاطر السيبرانية بين التحليل الكمي باستخدام نموذج FAIR والتقييم النوعي من خلال مصفوفة المخاطر. ولتحديد الأثر المالي للهجوم الإلكتروني، طُبّق نموذج توبين لقياس قيمة الشركة قبل الاختراق الأمني وبعده. وكشفت النتائج أن زين العراق لم تُفصح عن حادثة الأمن السيبراني في تقريرها السنوي، على الرغم من الخسائر المالية الفادحة التي تكبدتها. وهذا يُؤكد الحاجة إلى الشفافية وتشديد إجراءات الأمن السيبراني لضمان مرونة الشركات في العصر الرقمي.

الكلمات المفتاحية: تقنيات الحوسبة السحابية والأمن السيبراني وأنظمة المعلومات المحاسبية واستدامة الشركات.

1. Introduction

Rapid technological advancements have increased cyber threats, making digital systems more vulnerable to targeted attacks. The success of cyber attackers depends on their objectives, whether financial theft, data breaches, sabotage, or personal revenge. Hackers exploit system vulnerabilities to gain unauthorized access, leading to data destruction and record manipulation. This threatens the efficiency of electronic accounting systems and the accuracy of financial reports, negatively impacting corporate decision-making, productivity, and reputation. Ultimately, cyberattacks can result in significant financial losses and a decline in market value.

Based on the above, this research will be divided into the following sections:

Section One: Research methodology, previous studies, and the contribution of the current research.

Section Two: Theoretical framework on cloud computing technologies in accounting information systems, enhancing cybersecurity, and corporate sustainability.

Section Three: The impact of the adoption of cloud computing technologies on enhancing the cybersecurity of accounting information systems and their effect on corporate sustainability: Applied study on Zain Iraq Telecommunications Company (Al-Khatem).

Section Four: Conclusions and recommendations.

Lastly, the company's value pre-and post-exposure to cyber risks was measured using Tobins Q, a comprehensive metric of corporate valuation.

Section One: Research Methodology, Previous Studies, and the Contribution of the Current Research

1-1. Research Problem: With escalating speed of development in Cloud Computing technologies and growing company reliance on them, there exists a greater susceptibility to cyber threats that accounting information systems face. Along with those solutions for bettering cybersecurity come the challenges about the impact of such solutions on corporate sustainability. The research Question then begs how does adoption of cloud computing technologies in order to enhance cybersecurity affect accounting information systems? Will the adoption Windows CPU technologies positively or negatively impact corporate sustainability?

1-2. Research Importance

1. This study seeks to highlight the vital role played by cloud computing technologies in enhancing cybersecurity and protecting accounting data.
2. The research is intended to help companies make well-informed decisions with regard to investments in the new technologies.
3. The incorporation of cloud computing technologies allows for enhanced corporate sustainability through increased efficiencies and security for accounting information systems.

4. Provides support for scientific research on the relationship between technology and sustainability in a business environment.

1-3. Research Objectives: The research aims to study the relationship between adopting cloud computing technologies and enhancing the cybersecurity of accounting information systems, besides evaluating how this relationship affects corporate sustainability and putting forth recommendations to help companies improve their strategies to balance security and sustainability.

1-4 Research Hypotheses: Accordingly, and considering the research problem, significance, and objectives, and hence to achieve the intended goals, the researchers have formulated two main hypotheses for the present study, with three sub-hypotheses for each of these.

First: The first main hypothesis: "There is a statistically significant relationship between cloud computing technologies for enhancing cybersecurity in accounting information systems and corporate sustainability."

First sub-hypothesis: There exists a statistically significant relationship between cloud computing technologies and accounting information systems.

Second sub-hypothesis: There exists a statistically significant relationship between cloud computing technologies and corporate sustainability.

Third sub-hypothesis: There exists a statistically significant relationship between accounting information systems and corporate sustainability.

Second: The second main hypothesis: "There is a statistically significant effect of cloud computing technologies for enhancing cybersecurity in accounting information systems on corporate sustainability."

First sub-hypothesis: There is a statistically significant effect of cloud computing technologies on accounting information systems.

Second sub-hypothesis: There is a statistically significant effect of cloud computing technologies on corporate sustainability.

Third sub-hypothesis: There is a statistically significant effect of accounting information systems on corporate sustainability.

1-2 Importance of the Research

2. **Prior Studies:** In today's time, cybersecurity is becoming a very important field since people all over the world are dependent on electronic devices, the

systems of which are vulnerable to hacking, theft, and destruction. Considerable literary work is done on this area and focuses on various aspects. Some selected studies on how the use of cloud computing technology would benefit the accounting information systems of a financial company's cybersecurity issues are as such:

Ali & Khan (2020): The Impact of Cloud Computing on Accounting Information Systems – Evidence from SMEs. It suggests that cloud computing reduces costs and improves operational efficiency for small to medium-sized enterprises (SMEs).

Ng & Lau (2021): Cloud Adoption in Accounting: A Case of Emerging Markets. The study looked at cloud computing adoption in accounting information systems in emerging markets and talked about problems with security and privacy.

Zhang & Li (2022): The Role of Cloud-Based Accounting Systems in Improving Financial Reporting Quality: Examined how cloud-based accounting systems improve financial reporting quality, thus enhancing transparency and accuracy.

Brown & Adams (2020): Challenges and Opportunities in Adopting Cloud Computing in Public Sector Accounting Systems: Discussed the challenges in public sector accounting systems for adopting cloud computing and the opportunities available to them for improved efficiency.

Watkins (2014) and Tariq (2018): Focused on cyber-attacks and their effect on financial institutions, emphasizing that banks should do everything necessary to protect internal security by way of putting in place necessary measures, conducting cybersecurity audits, training employees in the use of modern technologies, and encrypting and scanning data from personal devices to ensure minimal losses.

Manisha et al. (2015): Cyber Risks in Online Banking: Review the study under view focused on cyber risks in online banking and the new techniques of hackers. The study underscored the prudent approach to training bank employees in secure online banking practices and how to safeguard their personal information when conducting online transactions**.**

Bassam & Alawi (2020): The Importance of Cybersecurity Systems in Risk Management in the Banking Sector: Identifies three classic types of

cybersecurity attacks, their rates of recurrence, and the role of organizational management to mitigate these cybersecurity threats by guaranteeing that adequate funding is put into measures of security and education of their employees with respect to potential threats. This research concludes that it is important to note that disclosure of cybersecurity risk reports has a positively meaningful consequence upon organizational risk management practices.

Hasani et al. (2023): Assessing Cybersecurity Adoption and Its Impact on Organizational Performance: The study offered a basis for further research and the possibility of IT and cybersecurity professionals adopting necessary technologies that project an affirmative effect towards organizational communication and improving performance of the companies adopting cybersecurity technology**.**

Olamide & Hassan (2023): The Impact of Accounting Information Systems on Financial Reporting Quality in Industrial Companies: In their study, they draw attention to the importance of a company having a high-quality AIS, which continually requires managing and operating updates of the involved hardware and software systems**.**

2-1. Differences Between the Current Study and Previous Studies: In reviewing a sample of previous studies that related to the management of cybersecurity risk, it became critical to determine the ways in which they differ from the current study. The studies that were reviewed generally addressed the following:

- ❖ Influence of cloud computing technology adoption on accounting information systems in small and medium-sized enterprises (SMES).
- ❖ Cloud computing helps raise the level of information quality and operational efficiency in financial reporting.
- ❖ Cybersecurity breaches and their effect on the banking sector, as well as mitigation strategies for these risks in banking and insurance.
- ❖ Data breaches and their effect on accounting information quality.
- ❖ Examining the cybersecurity adoption on organizational performance only.

In contrast, the current study addresses the financial sustainability aspects by focusing on how enhancing cybersecurity helps in corporate sustainability. It takes a critical look at understanding cloud computing technologies and cybersecurity, the risks they pose, their types and causes,

and how they are measured and assessed as to their severity. On the same note, it goes back to the design of accounting information systems, challenges they face, and stakeholder influence on corporate sustainability. This is especially addressed in establishing the corporate context of these studies held in publicly listed companies. 3. Theoretical Framework

3. Accounting Information Systems and Cloud Computing Technologies

3-1. Concept and Definition of Accounting Information Systems

- Computerized Accounting Information Systems (CAIS) constitute one of the basic pillars of support upon which management stands to execute its responsibilities. CAIS brings together accounting and information systems into a single unit. They integrate computer technology with human resources and accounting standards found usually in a business organization.
- The said integration enhances the availability of timely and accurate information pertinent to decision-making, guiding higher-level management to make the right decisions. Establishment and proper implementation of this system is a beneficial investment in the company's core focus activities and, hence, minimizes exposure to risks and human errors.

The computerized accounting information systems can also be described as "An integrated set of subsystems consisting of interrelated components, both tangible and intangible, that work in concert to process independently transaction data related to financial matters" (Firdaus, 2011). "It is also a system that collects, records, stores, and processes data to produce information for decision-making. It consists of people, procedures, instructions, data, software, IT infrastructure, internal controls, and security measures" (Marshal, 2018).

"Yet, it is also defined as a financial system that uses specialized automated devices, called calculators and computer systems, to collect, analyze, interpret, and present information to its users for decision-making" (Olatunji & Olusegun, 2021).

CAIS does its work by integrating many systems or key and subsidiary components, which constitute the architectural framework of the system. This architectural framework expresses its structural characteristics with respect to different stages and processes during the accounting cycle.

In addition to the primary and subsidiary components of computerized accounting information systems, the system requires a set of enablers to achieve its objectives. There are six essential components of accounting information systems: People, Data, Procedures and instructions, Software, IT infrastructure, Internal controls.

The design of a CAIS is tailored to meet the unique requirements of various financial and non-financial business activities, as companies primarily rely on accounting information systems to carry out their operations.

3-2 Cloud Computing Technologies: Cloud computing technologies are a means to support and develop accounting information systems. They provide infrastructure and technical resources such as servers, databases, and software that are accessed via the Internet. Cloud computing technologies refer to a set of tools and services that enable access to computing and technical resources through electronic devices.

These technologies allow companies to streamline operations, increase efficiency, and utilize computing resources more flexibly. They include various models such as IaaS, PaaS, and SaaS, along with other tools like cloud storage and serverless computing. These have been summarized by researchers as follows (Javaid & McGrath, 2022:13; McGrath & Walker, 2023:7):

1. **Infrastructure as a Service (IaaS):** Enables users to rent computing resources (such as servers, storage units, and networks) via the Internet.
2. **Platform as a Service (PaaS):** Provides a ready-to-use environment for developing and running applications without the need to manage the infrastructure.
3. **Software as a Service (SaaS):** Allows access to software applications over the Internet without requiring local installation.
4. **Cloud Storage:** Enables users to store and retrieve data remotely.
5. **Serverless Computing:** Allows code execution without the need to manage or allocate servers.
6. **Hybrid Cloud Computing:** Combines public and private cloud infrastructure, providing flexibility in managing applications and data.

7. **Private Cloud Computing:** Hosts cloud resources on infrastructure owned by the organization, without sharing them with other users.
8. **Cloud Security:** Refers to technologies and tools for protecting data and services in the cloud environment.

Additionally, Accounting Information Systems (AIS) rely on cloud computing technologies for several reasons summarized by researchers as follows: (Alghofaili & Tiron, 2024:19; Babarinde & Mousavi, 2023:10):

1. The ability to access data and systems from anywhere, at any time.
2. Cloud computing reduces maintenance and operational costs since resources are managed remotely.
3. Cloud computing services provide advanced levels of security and data protection.
4. Computing resources can be scaled to meet system requirements.

From the above, it can be concluded that cloud computing supports, develops, and enhances the efficiency of accounting information systems.

3-3. Cybersecurity Risks: Cybersecurity is essential in the digital age, serving as the foundation for protecting sensitive systems from breaches. As reliance on modern technology grows, its role becomes as vital as daily necessities. The National Institute of Standards and Technology (NIST) defines cybersecurity as "the protection of electronic communication systems and services, including the information within them, from damage." Meanwhile, the International Telecommunication Union (ITU) offers a broader definition, encompassing policies, tools, best practices, and technologies (Cifgi, 2022). Despite varying definitions, most align with the well-known threefold cybersecurity model.

- ❖ **Confidentiality** ensures that information remains inaccessible to unauthorized parties, extending the concept of privacy.
- ❖ **Integrity** guarantees data accuracy, completeness, and reliability.
- ❖ **Availability** ensures authorized users can access information whenever needed.

If a cyberattack succeeds, it can lead to data theft, espionage, or financial and privacy losses (Huang & Madnick, 2020). The 2020 Global Risks Report by the World Economic Forum highlighted cybersecurity as a

major global concern, with financial institutions being prime targets due to their reliance on digital systems (String & Welburn, 2022).

Key cybersecurity risk indicators include:

1. **Intent**: Determines whether a breach was accidental (e.g., employee errors) or intentional (for economic or non-economic motives).
2. **Origin**: Identifies whether the breach came from within the organization or an external entity for personal gain or data disclosure.

3. Classification Based on the Method of Cyberattack Execution:

Types of cyberattack include:

1. **Denial of Service (DoS/DDoS):** These cyberattacks intentionally overwhelm systems with excessive traffic, depleting resources and ultimately disrupting operations.
2. **Phishing:** Uses fraudulent emails to install malware or steal sensitive financial information.
3. **Eavesdropping:** Intercepting and filtering traffic within a network in a disruptive manner.
4. **Password Attacks:** Methods by which hackers assume a password or credential on a stolen leap, such as one guessed or based on brute force.
5. **SQL Injection:** Attacks that make use of transferring malicious code into the databases to steal confidential data.
6. **Malware**: Malicious software meant to infiltrate systems and damage them in some way, viruses and worms being the most popular examples.
7. **Zero-Day Attacks:** Exploits undiscovered system vulnerabilities when no fixes are out.

The major risk involved with cybersecurity is the lack of preventive measures, e.g., weak passwords and poor security tools (Kajawang, 2022). Financial institutions being older systems besides insufficient protection face somewhat extreme challenges, including risks that can affect their infrastructure, image, or finances. Proactive measures would greatly assist in managing these types of risks.

3-4 Company Sustainability: Companies seek to reach their primary goals while attaining the highest possible economic value-it mirrors their capability to make practical decisions and being sustainable. The company's value originates from expectations set by stakeholders regarding their

investments. The company's value is regarded as the primary indicator of its performance and financial position. A company's value is described as "the company's performance deduced through the analysis of its annual accounts" (Fen et al., 2012) or "the interpretations of investors and stock prices" (Susanti & Restiana, 2018). Such high stock prices can enhance the attractiveness of companies and instill a dream to make big bucks with an assurance of substantial profits. However, the value of the company also reflects the fact that it is capable of surviving and thriving; therefore, it becomes an important factor considered in making investment decisions and managing decisions (Kamalia, 2020).

3-6. Cybersecurity Risks on Accounting Information Systems and Their Impact on Company Sustainability: Cybersecurity risks impact accounting information systems and a company's valuation and worth by exploiting vulnerabilities to disrupt systems, steal information, or in some cases, manipulate information for misrepresentation. The risks thus introduced completely corrupt financial reports and tear down the warm bridge of trust established between clients and companies. This leads to enormous losses in financial terms due to recovery costs. It also has a negative impact on equity prices and reputations, thus posing a risk to the company's viability and future growth. The next figure explains the relationships.

Figure (1): The Relationship Between Study Variables

Source: Prepared by the Researchers

The researchers conclude that prioritizing cybersecurity and cloud computing technology can significantly enhance a company's sustainability and growth. These measures serve as protective barriers for sensitive and critical data, strengthening confidentiality, availability, and integrity. As a result, financial firms are encouraged to adopt advanced systems that fully comply with the necessary standards for sustainable growth.

4. **Data Analysis**: The researchers aim to measure the impact of cybersecurity risks on accounting information systems and the sustainability of Zain Iraq Telecommunications by analyzing its financial reports. These risks affect computerized systems by exploiting vulnerabilities due to the absence of necessary cybersecurity measures. Such vulnerabilities allow cyberattacks that disrupt systems, steal data, and produce inaccurate financial reports, ultimately weakening stakeholders' trust in the company.

   Adopting cloud computing technologies combined with cybersecurity measures contributes to enhancing data and network protection, ensuring information accuracy, and supporting the company’s sustainability and market value.

   4-1. Measuring and Presenting Zain Iraq Telecommunications' Commitment to Cybersecurity Measures: This entails the measuring and presentation of Zain Iraq Telecommunications commitment towards the cybersecurity system in 2021-2022. This is the period of the cyberattack on the financial wallet service for customers, with the assessment based on an analysis of its annual financial reports to show the effort taken in order to guarantee the existence of a safe electronic space for the systems.

   The Global Cybersecurity Index (GCI) is used here as a measure based on five criteria-\u2014it is a measure of the capability of the countries to combat cyberthreats along with their commitment towards the growth of the cybersecurity system.

Table (1): Measuring the five categories of the Global Cybersecurity Index (GCI), the research sample for the period 2021-2022.

Year				The Global Cybersecurity Index (GCI)
2022		2021		
Not Applied	Applied	Not Applied	Applied	
0	1	0	1	1- Legal measures: Laws and regulations related to cybersecurity crimes.
0	1	0	1	2- Organizational measures: The strategies used by the company to activate this area.
0	1	0	1	3- Technical measures: Addressing spam, detecting cyberattacks and responding.
0	1	0	1	4- Learning and growth measures: Awareness campaigns for individuals working through training courses for research and development in the field of cybersecurity.
0	1	0	1	5- Cooperation measures: Multilateral agreements for the public and private sectors and participation in international forums and associations.

Source: Prepared by the two researchers based on Zain Iraq data**.**

Table 1 shows cybersecurity measures and the level of compliance of Zain Iraq in implementing them.

Cybersecurity is crucial in both financial and non-financial reports. The annual reports (2021–2022) showed that the company achieved 100% compliance in cybersecurity measures to protect its systems from wiretaps, theft, and destruction. The risk of not implementing security measures was rated zero.

Despite strengthening its cloud and e-security portfolios, the company still faced a major breach. On August 27, 2022, a hacker launched a phishing attack on Zain Iraq, crashing the system for four hours and stealing 26 million Iraqi dinars from digital wallets. The breach, widely covered by media, likely exploited system vulnerabilities caused by negligence, complexity, or other cybersecurity gaps.

4-2. Measuring the Risks of Computerized Accounting Information Systems: It is very important to spot out the entire strength and weaknesses of the system by identifying the breach's root cause. Was it because of a loophole in the system, generally weak security awareness, or failure to update the system? What kind of attack happened?

To this end, two analysis and measuring tools will be applied.

4-2-1 Using SWOT Analysis to Identify Strengths or Weaknesses in the Accounting Information System of the Study Sample

SWOT Analysis is a tool used to identify and evaluate **Strengths (S)**, **Weaknesses (W)**, **Opportunities (O)**, and **Threats (T)** within a particular context. In the case of the security breach, SWOT analysis can be applied to the accounting information system (AIS) of Zain Iraq to identify internal and external factors impacting its cybersecurity.

This analysis involves examining the breach incident and asking targeted questions to uncover insights into each of the four elements of SWOT:[1] As shown in the following figure.".[2]

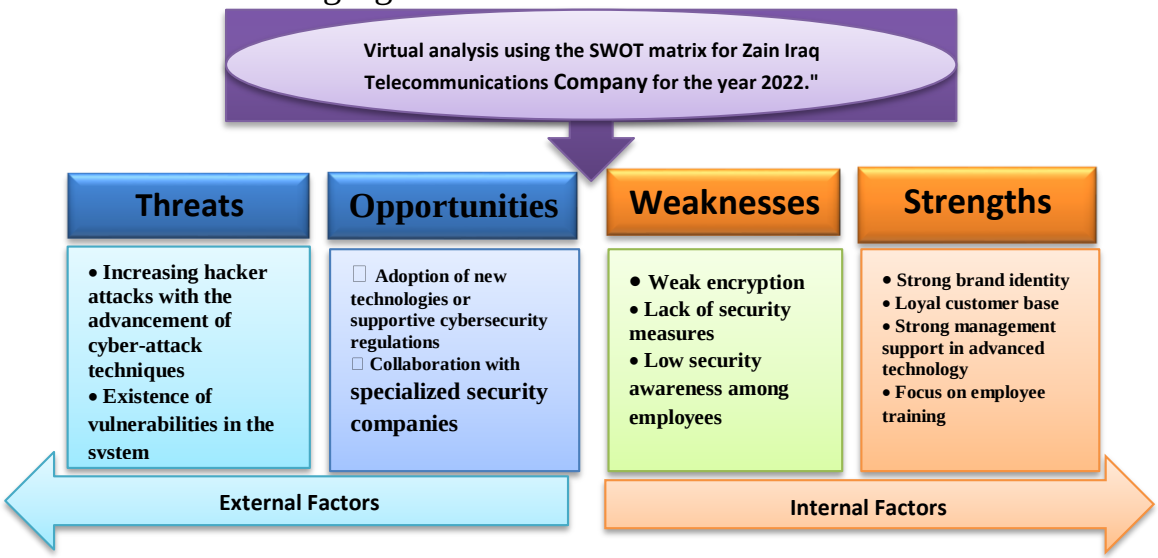

Figure (2): Virtual Analysis of the SWOT Matrix for the Research Sample for the Years 2021-2022

Source: Prepared by the researcher based on the website https://academy.hsoub.com/entrepreneurship/managementleadership

**"The news link is available through the following websites:

- [1] Shafaq News website: https://shafaq.com/ar/
- Al-Rafidain Channel: https://alrafidain.tv/47383/
- Al-Ghadeer Channel: https://alghadeertv.iq/archives/tag/"**

The figure presents a SWOT analysis of Zain Iraq for 2021 and 2022, highlighting its performance and interaction with internal and external environments. The company leveraged its strengths, such as infrastructure investment and employee skill development, to enhance services and market position. However, challenges like rising costs and security instability pressured profitability. Opportunities in the internet market and digital service demand helped counter threats.

Despite these efforts, cyber vulnerabilities remain a concern. Although no cyberattacks were reported in recent financial statements, financial systems are inherently at risk. Enhancing staff skills and applying OCTAVE Allegro risk assessments are crucial for addressing potential threats, as discussed in the next section.

4-2-2. OCTAVE Allegro Methodology for Assessing Risks in Automated Accounting Information Systems: OCTAVE Allegro is a comprehensive risk management framework designed to identify and assess security risks in information and communication technologies. It helps companies and individuals detect vulnerabilities and develop mitigation strategies without requiring extensive organizational involvement.

Unlike previous OCTAVE methods, Allegro focuses on critical information assets—how they are used, stored, transmitted, and exposed to threats. The approach follows eight steps across four key stages, as illustrated in the next diagram.

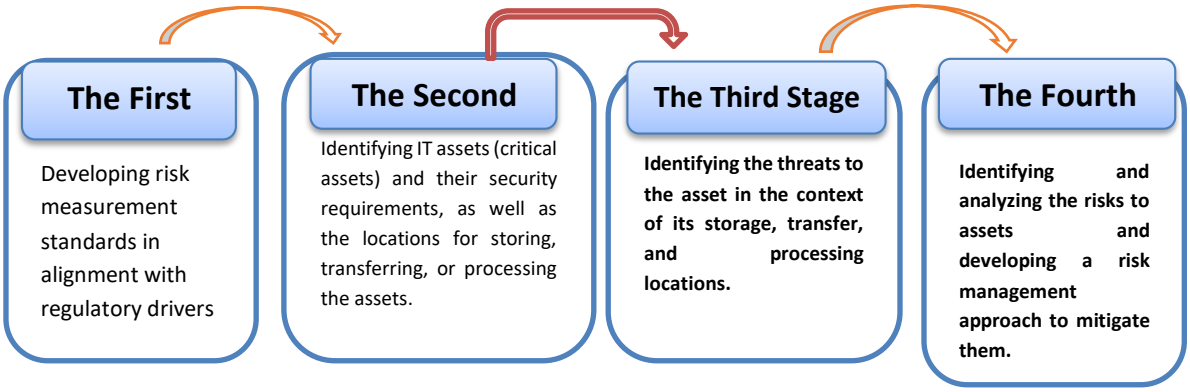

Figure (3):The Four Core Stages of the OCTAVE Allegro Methodology

Source: Based on available data from the official website. https://www.researchgate.net/publication/341156166 and adapted by the researcher

[3] Use of the OCTAVE Allegro methodology will allow those interested in risk assessment without requiring considerable organizational involvement or expertise. OCTAVE Allegro lays unusual emphasis on critical assets, the threats posed to such assets, the risk assessment, and finally strategies for minimizing the impact of such risks. The difference in this methodology, compared with previous OCTAVE methodologies, is primarily the focus on information assets in terms of how they are used, where they are stored, transmitted, and processed, and how they are exposed to threats, vulnerabilities, and disruptions.

Table (3)**:** Application of the Eight Steps of the OCTAVE Allegro Methodology for the Research Sample in 2022

OCTAVE Allegro Steps	Indicators Adopted from the Annual Reports of the Research Sample for 2022 and Circulated News	Results	Source
1. Define Scope and Objectives	Defining the systems and infrastructure to be evaluated for the research sample. The scope may include client portfolios and connected financial systems. The objectives include understanding the breach, identifying security vulnerabilities, and developing strategies to prevent future breaches.	Financial systems and servers connected to client portfolios were identified as the scope of evaluation. The objectives included understanding the breach and identifying vulnerabilities.	Circulated news and social media platforms

[3] **A video clip illustrating a cyberattack from previous years is available at the following link:**
https://www.youtube.com/watch?v=__kgKcvAtMc
* متاح عبر الموقع الالكتروني ** https://www.linkedin.com/pulse/what-octave-allegro-lazarus-alliance/
https://fedvte.usalearning.gov/publiccourses/FCRM/course/videos/pdf/FCRM_D01_S04_T01_STEP.pdf

OCTAVE Allegro Steps	Indicators Adopted from the Annual Reports of the Research Sample for 2022 and Circulated News	Results	Source
2. Identify Assets	Critical company assets include databases, financial systems, and servers. Asset descriptions: - Name: Customer Database. - Location: Specific servers (server system). - Importance: Storing sensitive customer data and financial transactions.	The customer database, financial system, and digital wallet servers were identified as critical assets. The critical asset for the research sample includes any program, server, or electronic code the attacker uses to reach the target (critical asset), which is the customer database.	Circulated news, social media platforms, and Zain Iraq's 2022 annual report
3. Identify Threats to Critical Assets	Threats include any type of cyberattack suitable for compromising the system, such as phishing, malware, undiscovered vulnerabilities, unintentional employee errors leading to data leaks, and insider attacks by trusted employees or partners misusing their privileges.	Several threats were identified, including phishing attacks, undiscovered vulnerabilities, malware, human errors, and insider attacks. The type of attack on Zain Iraq was phishing ("digital wallet compromise").	Circulated news and social media platforms

OCTAVE Allegro Steps	Indicators Adopted from the Annual Reports of the Research Sample for 2022 and Circulated News	Results	Source
4. Assess Risks and Prioritize	This phase involves analyzing risks and prioritizing them based on significance by evaluating impact and likelihood: - Impact: High (e.g., loss of customer data, service disruption), Medium (e.g., leakage of non-sensitive data), Low (minimal impact). - Likelihood: Frequent breaches indicate high likelihood; occasional breaches suggest medium likelihood, and rare breaches indicate low likelihood.	The impact was high (loss of customer data or service disruption), and the likelihood was medium due to multiple scattered breaches. The cyberattack was high-priority as it involved theft from customers' digital wallets.	Circulated news and social media platforms
5. Develop Mitigation Strategies	For each high-priority threat, corrective actions included enhancing cybersecurity, installing protection software, encrypting data, training employees, updating systems, and implementing strategies.	Zain developed mitigation strategies, including improving cybersecurity, training employees, and updating systems. Strategies were implemented to ensure system and data security.	Zain Iraq's 2022 annual report

OCTAVE Allegro Steps	Indicators Adopted from the Annual Reports of the Research Sample for 2022 and Circulated News	Results	Source
6. Create Execution Plan	Developing a detailed plan to follow up on implementing corrective measures, including system updates and employee training.	The plan included a timeline for implementing necessary strategies to address and mitigate risks.	Zain Iraq's 2022 annual report
7. Review and Update	Developing specific response plans for each risk, including preventive measures, emergency response procedures, and data recovery strategies in the event of an attack or breach.	Zain reviewed and updated plans based on feedback and new developments to manage risks and test effectiveness.	Zain Iraq's 2022 annual report
8. Evaluate Performance and Analyze Gaps	After developing and implementing risk response plans, procedures are established to periodically monitor and evaluate their effectiveness, ensuring expected performance and adjusting as needed.	Zain evaluated performance to monitor risk management plans and analyzed gaps between expected and actual performance. Gaps included the need for additional employee training in cybersecurity and insufficient security updates.	Zain Iraq's 2022 annual report

Source: Prepared by the researcher based on information obtained from the websites and annual reports of the research sample.

The table outlines the OCTAVE Allegro risk assessment for Zain Iraq's financial system breach in 2022, which resulted in a loss of 26 million Iraqi dinars. The attack, classified as a "digital wallet compromise" or "cryptocurrency compromise," exploited system vulnerabilities to illicitly withdraw funds, causing service downtime and data loss.

While the likelihood of recurrence is medium, the high impact makes this a critical cyber risk. Zain Iraq's risk management strategy focuses on strengthening cybersecurity through staff training and system updates to mitigate future threats.

4-5. Cyber Risk Measurement

4-5-1 Quantitative Cyber Risk Measurement Using the FAIR Model for the Case Study Sample (2021-2022): Quantitative risk analysis numerically assesses threats, vulnerabilities, and assets, such as financial data or electronic devices, to measure potential losses. The FAIR model, a globally recognized framework for information security risk, evaluates risk by determining asset value, loss frequency, and impact. It follows a four-stage process to quantify cyber risks, as illustrated in the diagram below.

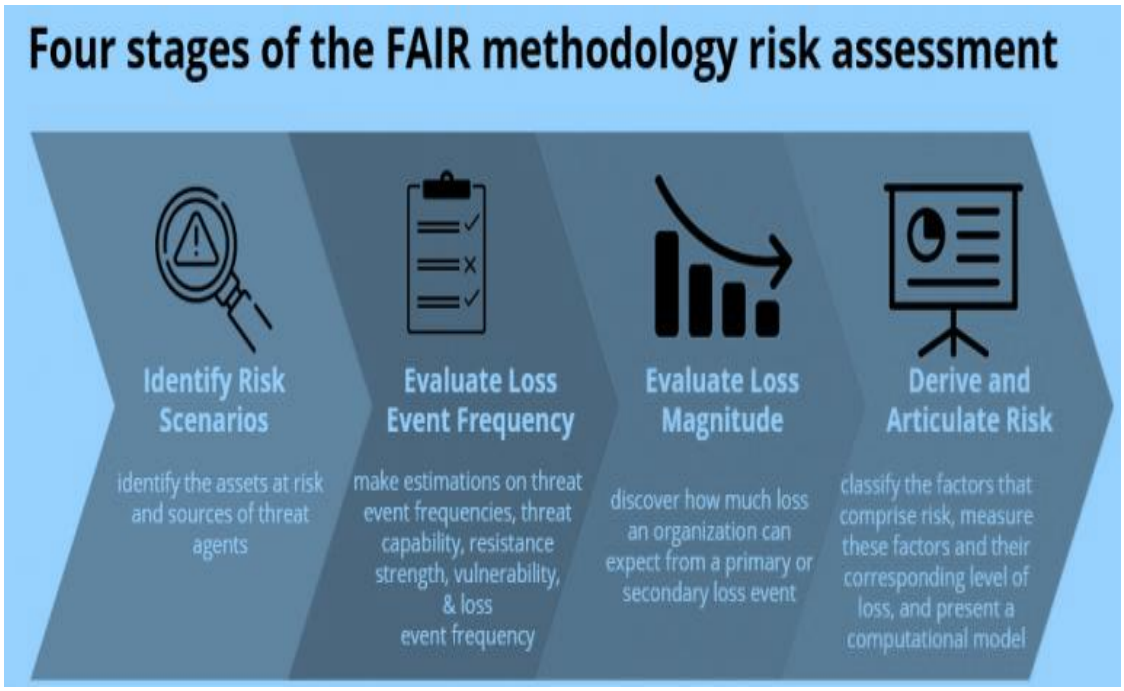

Fig 4. The four stages of cyber risk assessment according to the FAIR model for the 2021-2022 research sample

Source: Prepared by researchers based on FAIR Institute data to measure cyber **risks**https://www.fairinstitute.orgr

The diagram indicates the four stages of cyber risk, which can be further detailed by applying them to the case study as follows:

1. **Beginning Identification of the Assets at Risk and Sources of Threats Factors**: include the data retrieved from the case study from 2021 to 2022. The attack targeted Zain Iraq Telecommunications computer accounting system by an unknown cyber-hacker. The system was made down for four hours and a password attack was implemented by invading the code of the program and getting access to the customer database during the attack.
2. **Evaluating the Frequency of the Loss Event**: Data collection and estimates of the frequency of the event indicate that there was one breach on August 27, 2022.
3. **Quantifying Severity of Loss:** It is in this stage that the organization establishes the expected measure of loss coming from the primary or secondary loss event. From the gathered information regarding the breach, it was seen that a huge financial loss of 26 million Iraqi dinars imposed a foremost loss upon the company by being stolen from the wallets of customers, along with secondary losses that affected customers badly.
4. **Drawing Conclusions:** Overall risks are derived by giving the magnitude of loss and frequency of occurrence, both deriving the total loss figure as an output value through the following equation:

Risk = Loss event Frequency (In%) × Loss magnitude (In $)

The FAIR model equation can be applied for available data where the loss amount totals 26 million Iraqi dinars. For the frequency of the event, considering that it starts from 0% to 100%, 0% means building a probability that the attack has not taken place, gradually increasing frequency with subsequent values suggesting an increase in the likelihood of the event. The breach has happened only once; thus, it is represented by 10%, indicating that it has occurred once, depending on the risk equation defining the frequency for the risk starting from 10% to 100%. Following that, we will make the exchange of loss from Iraqi dinars to US dollars, apply the equation, and give the general outlook of the specific risk results. An equivalent of that loss in US dollars before the Iraqi stock exchange on August 27, 2022, during the actual breach, was approximately 1,470 IQD. This means that upon conversion, the loss amount in US dollars is approximately $17,687.74 as follows::

Risk =17687.74$×10%

$ 1768.7 =

4-5-2 Qualitative Assessment of Cyber Risk for the Research Sample for the Years 2021-2022: Determining the nature of cybersecurity risks against the qualitative assessment of risks is an analytical process that combines the purpose of estimating and understanding the potential possible risks the organization or even the system could face in the area of cybersecurity. This evaluation attempts to identify and assess vulnerabilities or gaps within software of systems, technologies, and processes that may be exposed to, or have already experienced, cyberattacks or unwanted activities.

The qualitative process of cyber risk assessment includes several key steps:

- **Identifying Assets:** The assessment starts with the identification of assets that are at risk from cyber threats. For the research samples, an asset is the computerized accounting system, which was already discussed in the previous quantitative measurement of the sample.
- **Identifying Threat Type:** At this stage, the notion of what type of threat could be damaging to the operating assets is decided upon. These threats can be different in a wide range. For the research sample conducted, the risk type is undermined as a method of a hacking attack known as a password attack characterized by an attacker overriding the password to access the system and steal the requisite data.
- **Evaluating Vulnerability:** This involves analyzing vulnerabilities in information systems or the possible protective measures, policies, and procedures that could be breached. Among other things, in this research sample under investigation, the revealed vulnerability exploited by the attacker may lie in the complexity of the system and, quite simply, the absence of the responsible employee able to cope with the complexity of its programs, coupled with the hacker's excellence in knowing the components of the system and how it works.
- **Estimating Risk:** Relying on the intelligence gathered through prior assessments, the estimated risk entails scoping out the potential negative impacts of the recognized threats against their chance of occurrence. In the present research sample, the incorporated risks could access the qualitative assessment of the collected and analyzed data, using the qualitative assessment matrix seen in the graph below.

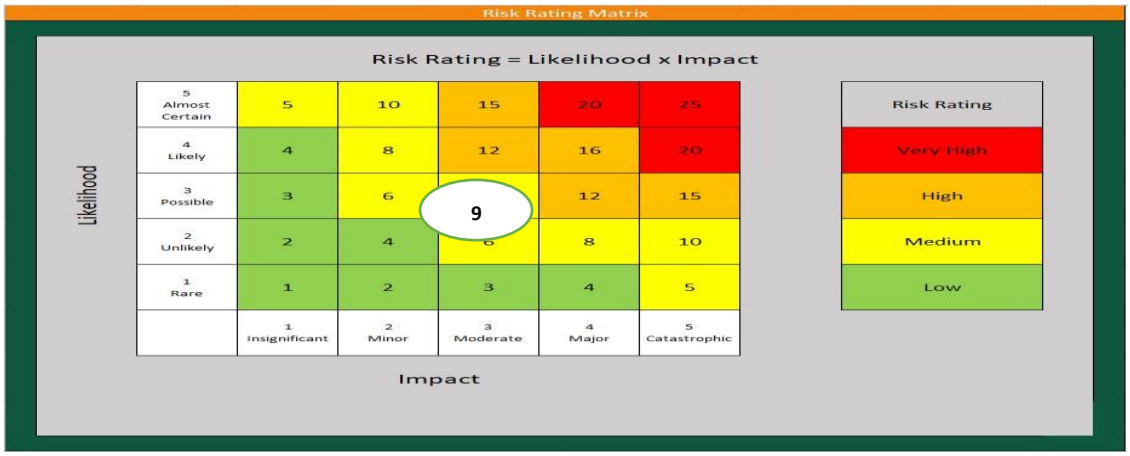

Fig5. Qualitative risk assessment matrix for the 2021-2022 research sample
Source: Prepared by the researcher based on Knoxville: 2024 https://policy.tennessee.edu.procedure

The colors in the table above represent the level of risk and the following table shows this

Table 4. Description of the effect of risk according to color for the color research sample

Color				
Effect Description	Low	Intermediate	High risk	Very High risk

Source: Table prepared by the two researchers The numbers (1-5) on the horizontal side of the above model symbolize
the description of probability, and the following table explains this.

Table (5): Description of the probability of the risk occurring

Degree	**1**	**2**	**3**	**4**	**5**
Probability Description	Rare	Unprobable	Possible	Probable	Confirmed

Source: Table prepared by the two researchers

The numbers (1-5) on the horizontal side of the above table symbolize a description of the impact of the risk, and the following figure explains this.

Table 6. Description of the degree of risk impact

Degree Range	**1-5**	**6-10**	**11-15**	**16-20**	**21-25**
Impact Description	Ineffective	Low effectiveness	Intermediate	Main	Disaster

Source: Table prepared by the two researchers

When applying the model to the research sample for the year 2022 at the time of the breach, we notice that the orange color, which expresses the presence of a high risk, is consistent with the event. As for the probability, the number 3 expresses an event that is somewhat confirmed. As for an impact, the number 3 expresses an event of medium consequence. In this manner, the risk can be expressed in magnitude according to the following equation.

Risk Rating = Likelihood x Impact **Risk Rating =**

$$3 \times 3 = 9$$

According to the equation and model, a breach to the Company's sample is classified as a medium-sized risk. The breach event aligns with an orange color at the degree of 15, per the above, thereby indicating the presence of a not insignificant risk due to the cyberattack, as the risk rate had reached approximately 15%, and the following equation explains this situation.

$$*\text{Impact ratio} = \frac{**\text{Loss amount}}{***\text{The total balance of customer accounts before the hack}} \times 100$$

$$IR = \frac{17687.7\$}{11{,}551{,}401\$} \times 100$$

$$IR = \%15$$

*=Impact ratio

**=Loss amount

***=Total customer account balance before hacking

6-3. Measuring the market value of Asia Cell and Zain Iraq: At year's end, the market value stock is that price that the stock is sold on the financial markets, which in brief, means the price that investors are willing to pay for the assets of a company. All times stock market price represents the actual trading price of the company's publicly traded shares on the stock exchange. The market value comes after the last day's closing price and is achieved by multiplying the share price by the number of shares on the last day From one trading day to one fiscal year, in its hypotheses.

Given that the relevant hypotheses and objectives of the inquiry define the market value of the company as the dependent variable for testing the hypotheses at hand, the researcher has set Tobin's Q model as the chief model to measure the company's value, following the approach of many articles focused on measuring market value. This model is recognized to provide

accurate results and has been widely used in the literature involving accounting and finance. The Tobin's Q ratio has been used extensively in the accounting and financial literature and is defined as:

Tobin's Q = Market Value of Equity + Book Value of Total Liabilities / Book Value of Total Assets

When the Tobin Q ratio is more than one, it means the market value of the assets exceeds the alternative value, the performance of the company is good, high profitability, and the stakes of the investment decision have paid off. So, there are chances that the investors will invest in that company. But if the Tobins Q ratio is less than one, it would mean that the market value is buying the assets less than their potential worth, which shows a poor company performance and unprofitability. Such a company may deter investors from investing .

Table 2. shows the year-on-year depreciation of the Zain Iraq market value in accordance with 2022 affiliation and the other data related to each other.

Table 7. Decline in the market value and company value of Zain Iraq, the research sample for the period 2021-2022

Fire Value	The Book value of total assets	The book value of total liabilities	The total market value of ownership rights	Number of shares (million shares)	The Market value	Years
52.1	4573866	2,744,083	4208501	1.829783	30,2	2021
51.1	4619604	2,789,821	4208501	1.829783	30,2	2022

Source: Table prepared by the researcher based on data from Zain Iraq, the research sample for the period (2021-2022).

Table 7 indicates that the value of Zain Iraq was the highest in 2022 at a value of 52.1 per share and its lowest value in 2022 at 51.1 per share, and according to Tobin’s Q scale, when the company’s value is less than one, this indicates that the market value of the assets is less of its replacement value, which means a decline in the company's good performance, profitability and successful investment decisions.

4-6 Inferential Analysis to Describe the Relationship Between Research Variables and Test Hypotheses

First: Methods of Data Collection: To achieve the research objectives and test its hypotheses, it was necessary to select an appropriate population for the practical application of the study. The research population comprised telecommunications companies in the local environment, and the research sample was chosen using a systematic random sampling method.

The research sample consisted of 92 questionnaire forms, which were distributed electronically through a dedicated link using the Google Forms platform. Table (8) presents the demographic characteristics of the research sample participants.

Table (8): Demographic Characteristics

Variable	Answer Alternatives	Number	Percentage
Age	Less than 30 years	15	16.30%
	From 30 to 40 years	38	41.30%
	From 41 to 50 years	27	29.35%
	More than 51 years	12	13.05%
	Total	92	100%
Degree	Diploma	14	15.22%
	Bachelor's	50	54.35%
	Master's	16	17.39%
	Ph.D.	12	13.04%
	Total	92	100%
Job	Cybersecurity Officer	8	8.70%
	Electronic Information Systems Manager	20	21.05%
	Electronic Information Systems Operator	21	22.10%
	Accountant in a Company	43	48.15%
	Total	92	100%
Professional Experience	Less than 5 years	9	9.78%
	From 5 to 10 years	24	26.09%
	From 11 to 15 years	30	32.61%
	From 16 to 20 years	16	17.39%
	21 years or more	13	14.13%
	Total	92	100%

Source: Prepared by the researcher based on the outputs of the (7SPSS.v2) program

A. Regarding the age group, the statistical results showed that the percentage of individuals aged 30 to 40 and 41 to 50 ranged between 29.35% to 41.30%, with a total of 65 individuals, representing the highest proportions. This indicates a significant reliance on the middle age group for managing functional tasks. On the other hand, the age groups below 30 years and above 51 years recorded a combined participation percentage of 13.04% to 16.30%, with 27 individuals falling within these categories.

B. Educational Level: The research sample indicates that most participants hold a bachelor's degree, accounting for 50 individuals or 54.35%. The remaining percentages varied, with 16 individuals holding a master's degree (13.04% to 17.39%), 14 individuals holding a diploma, and 12 individuals holding a doctorate.

C. Occupation: The demographic distribution of the study sample for occupational variables reveals that the category "Accountant in a company" recorded the highest percentage (48.15%), with 43 individuals participating in the questionnaire. Other categories, such as "Electronic Information System Manager" and "Electronic Information System Operator", were distributed between 21.05% and 22.10%, with a total of 41 individuals. Lastly, the "Cybersecurity Officer" category recorded a total of 8 individuals, accounting for 8.70% of the participants.

D. Work Experience: The statistical results indicate that the highest percentages were for the groups "5 to 10 years" and "11 to 15 years", which recorded participation rates of 26.09% and 32.61%, respectively, with a total of 54 individuals. These results suggest that the study sample has significant experience in their respective fields. Other groups were distributed with varying percentages between 9.78% to 17.39%.

Second: Testing the Normal Distribution of the Research Variables

To address the research questions and hypotheses, it is essential to ensure the normal distribution of data before presenting and analyzing the study results. The Kolmogorov-Smirnov Test was used to verify whether the data collected from the research sample followed a normal distribution, as shown in the table below.

Table 10: Results of the Normal Distribution Test

Variable	Kolmogorov-Smirnov Test Statistic	Test Parameter	Sample Size	Significance Value
Cloud Computing Techniques	0.1600	92	0.2200	Significant
Accounting Information Systems	0.1300	92	0.1340	Significant
Company Sustainability	0.1550	92	0.1870	Significant

Source: Prepared by the researcher based on the outputs of the (SPSS.v27) program

It is evident from the significance level of the Kolmogorov-Smirnov Test that the values for the variables were higher than 5%, indicating that the data follows a normal distribution. Therefore, the results obtained from the sample can be generalized.

Third: Reliability Test: This test is one of the essential conditions for validating the research instrument, highlighting its importance in ensuring the reliability of the tool (questionnaire). Reliability refers to the internal consistency of the measurement for the main research variables. Cronbach's Alpha coefficient is one of the most widely used measures for testing the reliability of a research instrument, as shown in the following table:

Table 11: Reliability Test

Variable	Cronbach's Alpha	Test Parameter	Number of Items
Cloud Computing Techniques	0.854	10	Reliability is Significant
Accounting Information Systems	0.863	10	Reliability is Significant
Company Sustainability	0.809	10	Reliability is Significant
The Questionnaire as a Whole	0.922	30	Reliability is Significant

Source: Prepared by the researcher based on the outputs of the (SPSS.v27) program

Table (18) shows that the Cronbach's Alpha values ranged between 0.809–0.863, which are greater than 70%. Additionally, the overall reliability of the questionnaire was 0.922, indicating that the study instrument has a good level of reliability.

3-3-2: Descriptive Statistics Procedures for the Research Sample: The process of presenting and discussing results requires the use of various tools and methods. To facilitate solving the research problem, the obtained data will be summarized in tables, analyzed, and interpreted to ensure accurate and easy comprehension of the results.

1. Cloud Computing Techniques in Enhancing Cybersecurity (Independent Variable)

Table (12): Descriptive Indicators for the Variable (Cloud Computing Techniques)

No.	Questions	Mean	Standard Deviation	Response Intensity
1	Cloud computing effectively contributes to improving cyber risk management for companies and protecting them from evolving threats.	4.09	0.709	81.80%
2	Cloud computing helps in continuously developing cybersecurity policies to keep up with modern threats.	3.92	0.768	78.40%
3	Cloud platforms are an effective means of enhancing cybersecurity awareness among employees through innovative training programs.	4.09	0.594	81.80%
4	Cloud computing contributes to better implementing international frameworks and standards for cyber risk management.	4.02	0.654	80.40%
5	Cloud systems enable protection of sensitive data	4.21	0.627	84.20%

	from leakage and ensure the security of companies' financial information.			
6	Cloud computing provides advanced security technologies like virtual firewalls and antivirus to enhance cybersecurity.	4.05	0.614	81.00%
7	Cloud computing enables regular security gap assessments and their effective and rapid correction.	4.12	0.742	82.40%
8	Using cloud computing tools contributes to recording and analyzing data for early detection of cyber threats.	3.78	0.587	75.60%
9	Cloud storage provides a secure backup system, protecting sensitive data from loss or breach.	4.15	0.581	83.00%
10	Having a specialized team supported by cloud tools enhances the ability to monitor and analyze security threats effectively.	4.07	0.483	81.40%
Total		4.05	0.635	81.00%

Source: Prepared by the researcher based on the outputs of the (SPSS.v27) program, as presented in the table above.

From Table (12), the highest and lowest agreement rates for the cloud computing technology variable statements can be summarized as follows:

A. The fifth statement, **"Cloud systems enable the protection of sensitive data from leakage and ensure the security of companies' financial information,"** recorded the highest level of agreement, with a mean of **4.21** and a standard deviation of **0.627**. The agreement intensity reached **84.20%**, highlighting the significance and role of cloud computing systems in

preventing data breaches by identifying and blocking any attempts to transfer or copy sensitive information outside the secure network.

B. The eighth statement, "The use of cloud computing tools contributes to recording and analyzing data for the early detection of cyber threats," recorded the lowest level of agreement, with a mean of 3.78 and a standard deviation of 0.587. The agreement intensity reached 75.60%, indicating the importance of cloud computing tools in logging all security events and user and system information, analyzing them to identify potential threats or risks at an early stage.

Accounting Information Systems Axis (The Mediating Variable)

Table (13): Frequencies, Percentages, Means, and Standard Deviations for the Variable "Accounting Information Systems"

No.	Questions	Mean	Standard Deviation	Response Strength (%)
11	The company relies on cloud computing in its accounting information systems to enhance the accuracy of financial and administrative data processing and assist management in making effective decisions.	3.92	0.677	78.40%
12	The company works on developing cloud-based accounting information systems to meet its needs and ensure compatibility with the latest technological advancements.	4.04	0.806	80.80%
13	The company prioritizes updating its cybersecurity in integration with cloud computing systems to enhance the effectiveness and efficiency of accounting information systems.	4.02	0.467	80.40%

No.	Questions	Mean	Standard Deviation	Response Strength (%)
14	The company provides necessary training for employees to efficiently use cloud-based accounting information systems, contributing to the overall performance improvement of the company.	4.12	0.604	82.40%
15	The company develops strategic plans for managing cybersecurity risks, integrating cloud computing to accelerate response and recovery from cyberattacks, enhancing accounting information systems.	4.03	0.558	80.60%
16	Continuous threats to the electronic system negatively affect the quality of produced information; however, cloud computing enhances the protection and reliability of this information.	4.13	0.685	82.60%
17	The company frequently faces hacking attempts on its electronic systems and accounting databases, but cloud computing systems reduce the likelihood of such breaches and provide advanced protection.	4.07	0.641	81.40%
18	The company's management acknowledges that information security risks can undermine users' trust in accounting information, but integration with	3.89	0.565	77.80%

No.	Questions	Mean	Standard Deviation	Response Strength (%)
	cloud computing increases security and confidence.			
19	The company has alternative solutions based on cloud computing to ensure the continuity of electronic systems in case of failures, providing uninterrupted information to users.	4.08	0.641	81.60%
20	The company's management includes additional information about cybersecurity risks related to cloud computing systems in its financial reports, enhancing transparency and trust between users and management.	3.97	0.508	79.40%
Total		4.027	0.6152	80.54%

Source: Prepared by the researcher based on SPSS v27 outputs.

From Table (13), the highest and lowest agreement rates for the (Accounting Information Systems) variable statements can be summarized as follows:

A. The sixteenth statement, "The continuous threats faced by the electronic system negatively affect the quality of the information produced; however, the use of cloud computing enhances the protection of this information and improves its reliability," recorded the highest level of agreement, with a mean of 4.13 and a standard deviation of 0.685. The agreement intensity reached 82.60%, emphasizing the importance of information quality, which can lose many of its attributes due to threats such as breaches and malware. These statistics highlight the positive role of cloud computing technologies in addressing and mitigating electronic breaches.

B. The eleventh statement, "The company relies on cloud computing in its accounting information systems to improve the accuracy of financial and administrative data processing and assist management in making effective decisions," recorded the lowest level of agreement, with a mean of 3.89 and

a standard deviation of 0.565. The agreement intensity reached 78.4%, reflecting the importance of providing accurate and reliable reports that enable the management to effectively track financial and administrative operations.

Company Sustainability Axis (The Dependent Variable)

Table (14): Statistical Indicators (Mean, Standard Deviation, Response Strength) for the Variable "Firm Value"

No.	Questions	Mean	Standard Deviation	Response Strength (%)
21	The company relies on cloud computing in its accounting information systems to enhance data security and improve financial and administrative operations, contributing to long-term sustainability.	4.587	0.538	91.74%
22	Cyberattacks can lead to the loss of sensitive data and disrupt operations, threatening the company's sustainability and undermining stakeholder trust.	4.370	0.675	87.40%
23	Developing cybersecurity risk management policies using cloud computing tools enhances the company's sustainability by improving its readiness to face future threats.	4.283	0.731	85.66%
24	Raising employees' awareness of cybersecurity through cloud-based training systems increases their ability to counter attacks, supporting the company's long-term sustainability.	4.109	0.818	82.18%

25	The company benefits from adopting international standards and frameworks for managing cybersecurity risks in cloud computing, enhancing its operational sustainability and reliability with investors and lenders.	4.489	0.620	89.78%
26	Data leakage prevention systems based on cloud computing help protect the company's valuable assets and reduce threats that could affect its sustainability.	4.446	0.600	88.92%
27	Technological measures, such as cloud firewalls and AI-powered antivirus software, ensure business continuity and enhance the company's sustainability.	4.272	0.878	85.44%
28	Periodic vulnerability assessments using cloud computing tools strengthen partners' and clients' trust in the company, supporting its long-term sustainability.	4.435	0.684	88.70%
29	Using cloud-based security event logging and analysis systems enables early detection of cyber threats, protecting the company's sustainability.	4.163	0.905	83.26%
30	A cloud-based backup system can reduce the company's potential losses during cyberattacks, supporting its financial and operational sustainability.	4.217	0.836	84.34%
Total		4.337	0.7285	86.74%

Source: Prepared by the researcher based on SPSS v27 outputs.

The descriptive statistics for the variable (Company Sustainability) from Table (14) indicate that most statements for the dependent variable (Company Sustainability) recorded high response levels and strong agreement by the study sample. The mean values for these statements ranged from 4.109 to 4.587, and the overall agreement level for the dependent variable was 4.337, reflecting a high level of agreement at 86.74%.

This percentage highlights the importance of enhancing employee awareness of cybersecurity and its role in reducing risks and increasing the long-term sustainability of the company. This contributes to increasing the company's value by adhering to international standards and frameworks in managing cybersecurity risks. Technological measures such as firewalls and antivirus programs have shown their contribution to maintaining business continuity and increasing company value.

Regarding the statements with the highest and lowest agreement levels based on response intensity, the following can be summarized:

A. The statement "The company relies on cloud computing in its accounting information systems to enhance data security and improve financial and administrative operations, contributing to long-term sustainability" received the highest agreement intensity at 91.74%. This value reflects the high agreement by the sample on the importance of relying on cloud computing to prevent cyber breaches, which can lead to sensitive data loss and operational disruptions. This reliance positively impacts the company's sustainability. The statistical indicators show a mean of 4.587 and a standard deviation of 0.538, indicating high consistency in responses.

B. The statement "Enhancing employee awareness of cybersecurity contributes to reducing risks and increasing the company's value in the long term" received the lowest response level at 82.18%. This value underscores the importance of raising employee awareness about cybersecurity in reducing risks and increasing the company's value over the long term. The mean for this statement was 4.109, with a standard deviation of 0.818, reflecting the level of response variability>

Note: For further clarification and to validate the study's hypotheses, additional details are included in the research appendix. These data and evidence support the findings, providing accurate documentation of the analyses and results. This strengthens the credibility of the study and reinforces its conclusions.

Key Findings:

- ❖ The importance of cybersecurity and cloud computing technologies is emphasized in enhancing the efficiency of accounting information systems by providing advanced protection for financial information, ensuring its integrity, reducing cybersecurity risks and costs, and enhancing transparency and trust between investors, partners, and stakeholders.
- ❖ These technologies contribute to improving the speed of response to attacks, recovery from them, and enhancing the quality of accounting data, leading to a positive impact on the overall company performance, financial stability, and market value in the modern digital environment.

Key Recommendations:

- ❖ Companies should adopt cloud computing technologies to enhance the security of their accounting information systems, providing advanced protection for financial data, ensuring quick response to cybersecurity attacks, and implementing effective recovery mechanisms. This will improve the quality of accounting outputs, increase investor trust, and enhance the company's market value.

Reference

1. Abu-Musa, A. (2005). Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations. Computer and Information Science, 18, 1-26.
2. Adeliza, A. (2017). Assessing the impact of computerized accounting system usage on organization performance in Tanzania: Case study on LGAS in Arusha Region. A dissertation submitted, Mzumbe University.
3. Alghofaili, M., Parast, A., & Tiron-Tudor, A. (2024). These authors discuss the flexibility and cost savings of cloud-based solutions in accounting, especially for collaborative work. They note that by providing real-time data access and automating routine tasks, cloud technology promotes better client relationships and enhances decision-making. Journal of Accounting and Cloud Technology.
4. Amidu, M., Effah, J., & Abor, J. (2011). E-accounting practices among small and medium enterprises in Ghana. Journal of Management Policy & Practice, 12(4), 146-155.
5. Appiah, O. A. (2014). Computerised accounting information systems: Lessons in state-owned enterprise in developing economies. School of Business, Kwame Nkrumah University of Science and Technology.
6. Babarinde, A., & Mousavi, M. (2023). This paper explores the impact of cloud-based accounting on data security and operational efficiency, particularly through the use of advanced encryption (Advanced Encryption Standard) and the necessity for secure data channels. Accountancy Age.

7. Canelón, J., Huerta, E., Leal, N., & Ryan, T. (2020). Unstructured data for proceedings of the 53rd Hawaii International cybersecurity and internal control. Conference on System Sciences.
8. Ciolan, I. M. (2010). Defining cybersecurity as the security issue of the twenty-first century: A constructivist approach. Published research, National University of Political and Administrative Sciences, Bucharest.
9. Fardinal. (2013). The quality of accounting information and the accounting information system through the internal control systems: A study on Ministry of State Agencies of the Republic of Indonesia. Research Journal of Finance and Accounting, 10(10), 1–14.
10. Hurt, R. L. (2013). Accounting information systems: Basic concepts and current issues (3rd ed.). New York, NY: McGraw-Hill/Irwin.
11. Javaid, I., Akindote, B., & McGrath, E. (2022). This study evaluates how cloud computing boosts efficiency, scalability, and data security in accounting firms. It highlights encryption and secure data protocols as vital for protecting financial data, while backup and disaster recovery ensure business continuity. Global Journal of Engineering and Technology Advances.
12. Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71-90.
13. McGrath, E., & Walker, D. (2023). This work covers challenges and privacy considerations, addressing how cloud systems meet diverse regulatory requirements like GDPR. They emphasize the importance of encryption and strict access controls to secure sensitive client data. International Journal of Accounting and Technology.
14. McLeod, R., & Schell, G. (2006). Management information systems (10th ed.). New Jersey: Prentice Hall.
15. Meiryani, M., Susanto, A., & Sudrajat, J. (2019). The effect of environmental complexity on the quality of accounting information systems: Integration flexibility and complexity dimensions. ICETT 2019: Proceedings of the 2019 5th International Conference on Education and Training Technologies, 115–119. https://doi.org/10.1145/3337682.3337702.
16. Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. Iraqi Journal For.
17. Mijwil, M., Filali, Y., Aljanabi, M., Bounabi, M., & Al-Shahwani, H. (2023). The purpose of cybersecurity governance in the digital transformation of public services and protecting the digital environment. Mesopotamian Journal of Cybersecurity, 1(6).
18. Ndubuisi, A. N., Chidoziem, A. M., & Chinyere, O. J. (2017). Comparative analysis of computerized accounting system and manual accounting system of quoted microfinance banks (MFBs) in Nigeria. International Journal of Academic Research in Accounting, Finance and Management Science, 7(2), 30-43.
19. Nisrina, I., Edward, I., & Shalannanda, W. (2016). IT governance framework: Case planning based on COBIT 5 for a secured internet service provider company. Case study.

20. Olatunji, C. O., & Olusegun, D. D. (2021). Computerized accounting system and performance of universities in Southwest, Nigeria. International Journal of Management (IJM), 12(5), 72-85.
21. Sage Software, Inc. (2020). Sage 50 accounting – US edition: User guide. Retrieved January from https://cdn.na.sage.com/docs/en/.
22. Saidin, S., & Badara, M. (2013). Impact of the effective internal control system on internal audit effectiveness at local government level. Journal of Social and Development Sciences, 4(1), 16.
23. Tejani, O. M. (2013). Computerized accounting information systems and perceived security threats in developing economies: The Nigerian case. Universal Journal of Accounting and Finance, 1(1), 9-18. https://www.researchgate.net/publication/351403544.
24. Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber-attacks on supply chain management systems. IFAC PapersOnLine, 48(3), 1846-1852.