Account and Financial Management Journal e-ISSN: 2456-3374
Volume 11 Issue 05 May 2026, Page No.- 4461-4471
DOI: 10.47191/afmj/v11i5.04, Impact Factor: 8.167

Cybersecurity and its Impact on Digital Accounting

Dr. Naji Shaib Al-Rikabi
Assistant Professor, Al-Bayan University, College of Business Administration, Accounting Department, Baghdad-IRAQ

ABSTRACT: The development in the field of artificial intelligence and information technology has forced accounting to move towards digital accounting in the present and perhaps towards smart accounting in the future. The result of the statistical analysis has shown beyond doubt that digital accounting cannot develop and continue without being protected by cybersecurity mechanisms and technologies, due to the many challenges and risks that financial institutions and individuals are exposed to, such as fraud, forgery, access to accounts, withdrawal of their balances, and hacking of accounts. It used a questionnaire consisting of two sections: the first section represents cybersecurity and includes 13 questions, while the second section represents digital accounting and also includes 13 questions. The sample size was fifty university professors specializing in accounting and other related fields to ensure they could answer the questionnaire questions accurately.

KEYWORDS: Traditional accounting, digital accounting, cybersecurity, cloud accounting, blockchain, information technology.

INTRODUCTION

Accounting practices in today's world are implemented through two approaches: the traditional approach, also known as conventional accounting, which relies on accounting principles, concepts, and objectives, and is executed manually or with basic computer use. The risks, threats, and challenges arising from this approach have been studied, and solutions have been developed through internal and external auditing, along with the accompanying evolution of auditing methods and techniques to meet these challenges. Despite the long experience with accounting and control procedures for fraud, manipulation, and forgery, breaches still occur that challenge internal control and auditing methods.

As for the digital accounting approach, it is based on the same concepts, principles, objectives and accounting practices, but the execution of accounting operations is done automatically or digitally using digital accounting tools such as cloud computing, artificial intelligence and blockchain, which are characterized by accuracy, speed and efficiency. In contrast, the challenges and risks of digital accounting differ radically from those in traditional accounting in terms of their comprehensiveness and scope, which requires new methods and tools to protect digital accounting information from fraud, forgery and manipulation. At the forefront of these methods is cybersecurity, and despite the development of its methods, many customer accounts in the world are exposed to theft of their balances, and this challenge continues between hackers and cyberattacks on the one hand, and designers of digital accounting systems on the other.

RESEARCH METHODOLOGY

Research Problem:

Traditional accounting faces the challenge of evolving and modernizing its work methods and transitioning to digital accounting. However, this digital transformation in accounting presents serious challenges, primarily maintaining the integrity and security of accounting information. This is especially true given that the entities using accounting information are not necessarily geographically close to the institutions themselves. Furthermore, the consequences of hacking and fraud can have a significant impact on various segments of society and may affect multiple countries simultaneously. Therefore, the digital transformation in accounting necessitates the protection and security of accounting information, particularly that related to the accounts and balances of companies, banks, and customers.

Research Objective:

This research aims to highlight the importance of digital accounting in saving time and effort, and in increasing speed and accuracy in completing accounting operations. Simultaneously, it emphasizes the importance of protecting digital accounting data from the serious threats and risks to which financial data is exposed. Here, the role of cybersecurity and electronic internal control procedures becomes crucial. These procedures include preventative, proactive, and corrective controls, and collectively, these tools provide a degree of protection for accounting data.

Research Hypothesis:

The risks and challenges of digital accounting, including fraud, forgery, manipulation, and unauthorized access, and

the resulting disastrous economic and social consequences for the balances and accounts of economic units and individuals, necessitate the use of cybersecurity technologies and methods to maintain the security and confidentiality of this information and prevent its theft.

Research Significance:

Digital accounting is a contemporary aspect of life in our world today. Therefore, research on this topic and other areas of digital life provides important insights into a world whose beginnings are taking shape and whose importance will increase in the near and distant future. future. This research topic is of great importance to specialists as well as the general public because of the shift towards digital accounting and the need to address threats and risks.

Research Methodology:

The research employs an analytical and inductive approach, utilizing a sample selection process and analyzing the responses of the sample members.

The Theoretical Framework Cybersecurity

The Concept of Cybersecurity: Cybersecurity is a set of tools, technologies, and practices designed to protect digital systems, such as digital accounting, from cyberattacks, unauthorized access, or theft. The use of cybersecurity has become essential due to the magnitude of the challenges facing accounting and financial operations and their impact on individuals and society.

Cybersecurity objectives:

1. To maintain the confidentiality of information and protect it from unauthorized access.
2. To ensure the integrity of data and prevent tampering, theft, or unauthorized alteration.
3. To ensure secure access to all systems and services available to authorized users.

Cybersecurity Areas:

Cybersecurity contributes to protecting a wide range of digital systems, software, and various electronic devices, including:

- Network Security: Cybersecurity helps protect networks from hacking, attacks, and viruses.
- Application Security: Cybersecurity, along with other systems, helps protect against malware that infiltrates accounting information and software to steal, manipulate, or alter its course.
- Data Security: Cybersecurity, along with other systems, plays a crucial role in protecting data during storage, transmission, and processing.
- Terminal Security: Cybersecurity, along with other systems, plays a vital role in protecting phones and computers from hacking and preventing damage to their software and hardware.
- Incident Response: Cybersecurity and other systems play a crucial role in handling security incidents and mitigating their damage. This is evident in the numerous protection systems for software, data, and operating systems. (Alvina Y., & others, 2024, p: 48-53)

Areas of Cybersecurity Application in Digital Accounting

First: Protecting Accounting Databases:

- This involves protecting customer, supplier, employee, and transaction databases from forgery, manipulation, and misuse.
- Using data and information encryption techniques and securing access control to accounting databases.

Second: Securing Cloud Accounting Systems:

- Using applications such as QuickBooks Online and Xerox.
- Ensuring the confidentiality of financial data stored in the cloud.

Third: Protection Against Financial and Electronic Fraud:

(Abu-Dabaseh & Others, 2025, p. 400)

- Detecting attempts to manipulate accounting data.

Areas of Cybersecurity Application in Digital Accounting

First: Protecting Accounting Databases:

- This involves protecting customer, supplier, employee, and transaction databases from forgery, manipulation, and misuse.
- Using data and information encryption techniques and securing access control to accounting databases.

Second: Securing Cloud Accounting Systems:

- Using applications such as QuickBooks Online and Xerox.
- Ensuring the confidentiality of financial data stored in the cloud.

Third: Protection Against Financial and Electronic Fraud:

(Abu-Dabaseh & Others, 2025, p. 400)

- Detecting attempts to manipulate accounting data.
- Using data analytics and artificial intelligence techniques to detect suspicious patterns.

Fourth: Protecting Enterprise Resource Planning (ERP) systems:

- Using software such as Oracle, SAP, and others.
- Protecting accounting systems in economic units from cyber threats.

Fifth: Protecting electronic transactions and financial reports:

- Protecting accounting processes such as sending financial reports and accounting correspondence via email or WhatsApp.
- Protecting documents from theft, manipulation, fraud, and forgery.

Sixth: Ensuring compliance with security standards and policies:

- Adhering to ISO/IEC 27001 standards for information security management.
- Adhering to SOX or GDPR regulations that affect accounting data.

Seventh: Protecting accounting terminals:

- Protecting computers and phones used by accountants to access financial data.

Eighth: Protecting AI-based accounting software:

- Protecting AI applications from attacks that affect accounting processes and financial forecasting. Economic units that use a cloud accounting system and artificial intelligence in analyzing accounting data usually use cybersecurity tools to encrypt data, determine access privileges to databases, take backups periodically, and analyze user behavior to detect hacking attempts.

Cybersecurity techniques are a set of tools and methods designed to protect digital systems, networks, software, and data from cyber threats such as hacking, malware, theft of financial assets, and unauthorized access to company and customer accounts. The most important of these techniques are listed below (Hasan, & others, 2024, pp. 68-70):

First: Firewalls. These act as a barrier between external influences on the computer's internal network and the internet, preventing unauthorized access. Firewalls are designed as part of the computer's internal control systems.

Second: Encryption. This involves converting accounting data into unintelligible codes to prevent espionage or theft. Several methods exist for this purpose.

Third: Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These systems are used to detect and prevent intrusion attempts into the computer system and are known as proactive electronic security.

Fourth: Multi-Factor Authentication (MFA). This requires more than one security measure to prevent access to the computer, such as a password and a code sent to a mobile phone.

Fifth: Backup Technologies. These are used to protect accounting data from damage, theft, malfunctions, or corruption.

Sixth: Identity and Access Management (IAM). This technology controls who can access important accounting systems and data.

Seventh: Secure Cloud Computing. This technology is used to securely store accounting data in the cloud with a high level of protection.

The Theoretical Framework of Digital Accounting

The concept of digital accounting is one of the contemporary methods that relies on modern technologies such as cloud accounting, artificial intelligence, and blockchain to automate accounting operations, such as recording in accounting books, classifying in the general ledger, analysis, and preparation of financial reports, instead of traditional manual or paper-based methods. (Kuntoro, A., & YKPN, P., 2025, P: 753-754)

The Historical Development of Digital Accounting

The emergence of digital accounting is a result of two main factors: the nature of traditional accounting, which evolves and responds to societal needs, and the tremendous technological advancements. In brief, the stages of accounting development can be summarized as follows:

Stage One: Traditional Manual Accounting, which appeared before the 20th century. This involved paper journals and ledgers, single-entry bookkeeping, and later double-entry bookkeeping. All accounting operations were performed manually, were relatively slow, and prone to human error. This stage is complex because it was used in widely separated periods, including the Sumerians, Babylonians, and the Islamic civilization.

Stage Two: Mechanical Accounting, which began in the early 20th century with the advent of mechanical counting and calculating machines, such as the Burroughs calculator. These machines reduced manual effort and human error.

Stage Three: Computerized Accounting, which began in the 1950s. This marked the beginning of the digital transformation, with the use of mainframe computers to process accounting data. Software related to accounting systems emerged, but the hardware and software were expensive and required highly skilled personnel to operate.

Stage Four: This stage began in the 1980s and extended into the 1990s. Commercial accounting software became widespread, and personal computers (PCs) were used. It became possible to process accounting activities, from sales and expense reports to the preparation of financial statements, automatically in both small and large companies. This represents the true beginning of digital accounting, coinciding with the emergence and widespread use of the internet.

Stage four: Integrated Digital Accounting. This stage began in 2000 and continues to the present. Enterprise Resource Planning (ERP) systems such as Oracle Financials, SAP, and Microsoft Dynamics emerged, and accounting software evolved into cloud-based accounting systems. Accounting data became accessible from anywhere in the world, allowing for file sharing with accountants and automatic system updates. This stage also highlighted the need for electronic data protection measures, such as cybersecurity, as well as electronic internal control tools.

Stage five: Smart Accounting. This is the next generation of accounting and is expected to extend from 2020 to 2030. The focus in this stage is on artificial intelligence, machine learning, and blockchain in:

- Big Data Analytics
- Financial Forecasting
- Full Automation of Routine Processes
- Advanced Protection of Accounting Data Using Blockchain (Ali & Hassan, 2021, pp. 12-15)

Key Characteristics of Digital Accounting:

1. Adoption of automated accounting software such as QuickBooks, Oracle, SAP, and other programs that automate accounting processes.
2. Automation automates accounting processes such as preparing sales lists, financial statements, and calculating taxes, reducing errors and saving time.

3. Cloud Accounting: Storing accounting data and information online allows easy access from anywhere, enhancing collaboration and accessibility.
4. Big Data Analytics: Using artificial intelligence and data analysis to provide more accurate financial reports and forecasts.
5. Integration with other programs within the economic unit, such as linking accounting systems like sales, inventory, or human resources systems.

Benefits of Digital Accounting:
1. Saving time and effort, ensuring the accuracy of accounting information, and reducing human error.
2. Improving the ability to make sound strategic decisions.
3. Providing quick and immediate access to financial data and speeding up the preparation of financial reports.
4. Reducing costs by minimizing the need for manpower.
5. Providing better protection for data and information. (Hassan & Ali, 2021, pp. 84-86)

Comparison between Digital and Traditional Accounting

Standard	Digital Accounting	Traditional Accounting
Tools	Software and smart applications	Manual paperwork and data entry
Accuracy	High accuracy due to high automation	Subject to human error
Speed	Very fast or instant response	Relatively slow
Data analysis	Advanced using artificial intelligence	Limited
Access to information	Cloud-based and accessible from anywhere	Local and limited

Digital Accounting Applications
1. Cloud-based accounting software such as QuickBooks, Xerox, and others.
2. Artificial intelligence for data analysis and financial forecasting.
3. Blockchain technology for securing accounting transactions and preventing fraud.
4. Automated accounting systems for processing receivables and payments.
5. Accounting robots for automating routine tasks. (Zebua W., 2025, p: 591)

Contemporary Trends in Digital Accounting

Global trends in digital accounting reflect rapid technological advancements and the drive of economic units towards digital transformation to achieve efficiency, accuracy, and transparency. The most prominent trends in digital accounting are as follows:

First: The increasing reliance on artificial intelligence and machine learning through the adoption of the following activities:
- Using artificial intelligence to analyze financial data and predict trends.
- Automating repetitive tasks such as data entry, bank account reconciliations, and financial reporting.
- Assisting in the detection of fraud, forgery, and financial risks.

Second: Advanced analytics and Big Data Analytics through the adoption of the following activities:
- Analyzing big data for a deeper understanding of customer behavior and analyzing market trends and consumer preferences.
- Adding value to decisions based on real-time and direct analysis of financial data.

Third: Reliance on Cloud Accounting through the adoption of the following activities:
- Cloud accounting systems provide flexible access to data from anywhere.
- Reducing the costs of traditional infrastructure. - Automatic updates and integration with other systems, as seen in computer and smartphone system updates.

Fourth: Utilizing Blockchain technology through the following activities:
- Enhancing transparency and security in financial and accounting transactions.
- Using smart contracts in accounting transactions.
- Providing immutable records, thus facilitating auditing processes.

Fifth: Automation and software robots through the following activities:
- Using robots to perform routine accounting and auditing tasks with high accuracy.
- Speeding up accounting operations and reducing human error.

Sixth: Cybersecurity and Digital Accounting through the following activities:
(P: 205-206) 2025 Aisyah & Tjandrakirana,)
- Due to the digital storage of sensitive financial data, cybersecurity has become vital.
- Focusing on data encryption, advanced authentication systems, and continuous automated monitoring. Seventh: The Accountant's Role as a Strategic Analyst through the following activities:
- Shifting the accountant's role from simply recording accounting data to becoming a financial and analytical advisor using advanced digital tools.
- The need for accountants to possess analytical and technical skills in addition to traditional accounting knowledge.

Eighth: Integration between Financial and Technical Systems through the following activities:

- Integrating accounting systems with human resource planning systems.
- Unifying databases and linking financial operations with production, inventory, human resources, control, and auditing.

Ninth: International Digital Accounting Standards through the following activities:

- Using Extensible Financial Reporting Language (EFRL) to facilitate the electronic exchange and analysis of financial data.
- Supporting transparency and standardized accounting reporting at the international level.

The Relationship Between Digital Accounting and Cybersecurity

Digital accounting and cybersecurity are closely linked in light of the current development in the field of digital accounting, which relies on technology to analyze and record accounting transactions. Cybersecurity, on the other hand, focuses on protecting accounting systems and data from cyber threats. Digital accounting increasingly uses electronic systems and modern technologies such as cloud computing, artificial intelligence, and blockchain technologies. With this transformation, cybersecurity has become an imperative to prevent cyber threats such as hacking and electronic fraud. A prime example of this is the fraud that customers who use Visa cards and other electronic payment methods are exposed to. This necessitates strong security measures to protect financial data from all directions. Digital accounting tools can also help in detecting financial fraud and advanced analyses that suggest the presence of security threats. Therefore, there is an integration between the work of digital accounting and cybersecurity to ensure the safety and security of financial data. Linking cybersecurity to digital accounting is of paramount importance, as the digital transformation in accounting has made financial data vulnerable to cyber threats, necessitating effective protection through cybersecurity technologies and practices. The following are areas of linking cybersecurity to digital accounting:

1. Protecting sensitive accounting data, including assets, revenues, expenses, customer bank account numbers, and other information. To protect this data: (Shchyrba I., & Others (2024), p: 449)

- Digital accounting relies on the storage, analysis, and processing of financial data.
- Encrypting accounting data and preventing unauthorized access to accounts are important cybersecurity tools.

2. Ensuring integrity and reliability: Cybersecurity protects the accuracy of accounting information and prevents manipulation or unauthorized alteration of electronic accounting records:

- Avoiding the deletion of digital accounting data without proper authorization leads to misleading financial reports.
- Cybersecurity ensures data integrity through the adoption of auditing and authentication systems.

3. Detecting fraud and financial manipulation through:

- The use of artificial intelligence in cybersecurity helps in the early detection of suspicious activities in accounting systems. An example is an automatic alert system for unusual money transfers.

4. Compliance with standards and regulations: Numerous regulations, such as GDPR in Europe and SOX in the US, impose strict protections on accounting data. Cybersecurity is a fundamental part of this compliance, as many economic entities adopt regulations to protect financial data, such as the Financial Regulation for the Protection of Data in Accounting Units. These regulations lead to compliance through data access control and protection systems.

5. Countering internal threats originating from employees within the economic entity who aim to falsify financial data, and external threats represented by cyberattacks and breaches.

Studying the Relationship Between Digital Accounting and Cybersecurity

First: Data Collection Methods

To test the research hypothesis, a questionnaire was designed consisting of two sections. The first section measured the impact of the cybersecurity variable on the digital accounting variable and comprised thirteen questions. The second section focused on the use of digital accounting mechanisms and also consisted of thirteen questions. Twenty-five questionnaire forms were used, and a five-point Likert scale was employed.

Second: Describing the General Information of the Research Sample

Table (1) shows the description of the research sample in terms of certificate and academic title

Academic title / Certificate	PhD	Certified Public Accountant	MSc	Diploma	Total
Prodessor	5	1			6
Assistant professor	9	1			10
Lecture	14				14
Assistant Lecture	12		7	1	20
Total	40	2	7	1	50

Table No. (1) shows that the percentage of PhD holders, Higher Institute of Accounting certificate, Master's degree, and Higher Diploma is 64%, 0.4%, 28%, and 0.4% respectively, and the percentage according to the academic title, Professor, Assistant Professor, Lecturer, Assistant Lecturer is 1.2%, 4%, 1.6%, and 3.2% respectively. This means that the researcher relied on a sample of specialists in the field of accounting, business administration, and other specializations, and their answers were useful, and the statistical analysis of the research was based on them.

Third: Questionnaire Validity and Reliability Test:

The following tests were conducted on the questionnaire to verify its validity and reliability:

1- Content Validity Test.

This refers to the questionnaire's ability to express the purpose for which it was designed. There are several methods for measuring questionnaire validity, the most important, common, and accurate of which is the comparison of extreme groups. This method involves arranging the questionnaire results in ascending order and dividing them into two groups. The 27% with the highest scores are selected as the first group, and the 27% with the lowest scores as the second group. The t-test is calculated according to the following formula:

$$t = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

They are the mean of the first group and the mean of the second group, respectively. $\bar{x}_2, \bar{x}_1$

They are the variance of the first group and the variance of the second group, respectively. S_2^2, S_1^2.

Then we compare the calculated t-value (7.25) with the tabulated t-value (1.645) at a significance level of 0.05 and degrees of freedom (1.28). If the calculated t-value is greater than the tabulated t-value, there are differences between the two means, and the questionnaire is valid in its measurement; otherwise, the opposite is true.

2- Questionnaire Reliability Test

Reliability means that the questionnaire measure gives the same results when applied to the study population after a period of time. There are many statistical methods to determine the reliability of a questionnaire measure, and they all rely on the concept of the correlation coefficient. One of the most important, valid, and commonly used formulas is Guttmann's formula.

$$R = 2(1 - \frac{S_1^2 + S_2^2}{S^2})$$

Reliability coefficient (R)

Variation of scores for odd-numbered questions

Variation of scores for even-numbered questions

Variation of scores for all questions

Table. (2) shows the results of validity and reliability coefficient

the questionnaire	Calculated (Truth) t	stability coefficient R
Cybersecurity	**0.79**	**8.33**
Digital accounting	**0.83**	**8.26**
Total	**0.82**	**8.30**

The critical validity test value was 1.645, while the calculated value was greater than the critical value, confirming the validity of the questionnaire. Furthermore, the reliability coefficient was greater than 0.5, further confirming the reliability of the questionnaire.

3- Testing the extent of difference in the research sample's opinions when answering the questionnaire questions.

Table (3) illustrates the degree of difference in the research sample's opinions regarding each of the questionnaire's axes. The coefficient of difference for the cybersecurity axis was 6.6057, while the coefficient of difference for the digital accounting axis was 6.8976. The similarity in the coefficients of difference between the two axes is attributed to the homogeneity of the research sample and their shared perspective on the research topic.

Table (3) shows the extent of the difference in the opinions of the research sample when answering the questionnaire items.

Research topics/scale	Arithmetic mean	Standard deviation	Coefficient of variation
Cybersecurity	**4.34**	**0.657**	**6.6057**
Digital accounting	**4.38**	**0.635**	**6.8976**

Fourth: Analysis of the Research Sample's Responses.

1- Arithmetic Mean, Standard Deviation, and T-Test.

Table (4) shows the analysis of the research sample's responses regarding the cybersecurity axis. The arithmetic mean for this axis ranges between 28.386 for the second question (Are you familiar with cybersecurity techniques applied in digital accounting?) and 39.102 for the first question (Do you encourage the dissemination of the

cybersecurity concept?). The analysis reveals a divergence of opinions regarding whether or not to encourage the dissemination of the cybersecurity concept. The researcher believes that the reason for this difference is primarily due to the relative novelty of the topic.

Table (4) Arithmetic mean, standard deviation and T test for the cybersecurity axis.

Sequence	Details	Arithmetic mean	Standard deviation	T-test
1	Do you encourage the spread of the concept of cybersecurity?	39.102	0.581	39.102
2	Do you have a grasp of the cybersecurity techniques applied in digital accounting?	**28.386**	**0.726**	**28.386**
3	Would you prefer to receive training or attend a cybersecurity workshop in recent years?	**34.322**	**0.510**	**34.322**
4	Are strong, regularly changed passwords used to access digital accounting files?	**29.032**	**0.653**	**29.032**
5	Do you use two-factor authentication when accessing digital accounting files?	**29.698**	**0.737**	**29.698**
6	Is accounting data encrypted during transmission and storage?	**29.044**	**0.707**	**29.044**
7	Is the accounting data backed up daily, weekly, or monthly, and automatically?	**29.044**	**0.702**	**29.044**
8	What are the main threats to your digital accounting data? - Cyberattacks - Malware - Internal data leaks - Human error	**29.305**	**0.723**	**29.305**
9	Do you believe that current cybersecurity measures are sufficient to protect digital accounting data?	**34.082**	**0.645**	**34.082**
10	How does weak cybersecurity affect the accuracy of financial reports?	**38.570**	**0.586**	**38.570**
11	Has the implementation of cybersecurity measures in your economic unit contributed to reducing incidents of hacking and cyber intrusion?	**39.102**	**0.581**	**39.102**
12	In your opinion, what are the priorities for developing cybersecurity in digital accounting? - Employee training - Software updates - Strengthening encryption procedures - Increasing the cybersecurity budget	**28.386**	**0.726**	**28.386**
13	In your opinion, what is the most important role of cybersecurity in digital accounting? - Protecting data confidentiality - Ensuring data integrity - Ensuring business continuity - Complying with regulations	**34.322**	**0.510**	**34.322**

Table (5) shows the analysis of the research sample's responses to the digital accounting axis, as the arithmetic mean ranges between 4.20 for the eighth question (Does senior management encourage the shift to digital accounting?) and 4.60 for the first question (Do you have a clear understanding of the concept of digital accounting?). The analysis shows that the research sample's opinions agree with what the researcher put forward about the role that digital accounting plays in achieving efficiency, speed and accuracy in completing accounting operations.

Table (5) Arithmetic Mean, Standard Deviation, and T-Test for the Digital Accounting Axis

Sequence	Details	T-test	Standard deviation	Arithmetic mean
1	Do you have a clear understanding of the concept of digital accounting?	**46.000**	**0.500**	**4.60**
2	Do you have any idea about the technologies and tools used in digital accounting (e.g., systems, cloud, electronic signatures) ERP	**31.360**	**0.714**	**4.48**
3	Does digital accounting differ fundamentally from traditional accounting?	**34.441**	**0.627**	**4.32**
4	Does digital accounting improve the accuracy of financial data?	**31.960**	**0.663**	**4.24**
5	Does digital accounting speed up financial reporting and reduce accounting errors?	**44.322**	**0.510**	**4.52**
6	Do you have confidence in the security of electronically stored financial data?	**27.033**	**0.792**	**4.28**
7	Are the procedures for controlling access to accounting data dual?	**31.553**	**0.678**	**4.28**
8	Does senior management encourage the shift to digital accounting?	**32.533**	**0.645**	**4.20**
9	Are there the necessary infrastructures, including personnel, equipment, and software, for digital accounting?	**31.143**	**0.700**	**4.36**
10	Is a lack of technical expertise hindering the shift towards digital accounting?	**32.533**	**0.645**	**4.40**
11	Does the financial cost of adopting digital accounting pose a barrier for economic units?	**31.143**	**0.510**	**4.48**
12	Does the economic unit provide sufficient training for the use of digital accounting systems?	**46.000**	**0.500**	**4.60**
13	Does digital accounting better support decision-making?	**31.360**	**0.714**	**4.48**

Note: The significance level for all t-values is P=0.000 for each question in both axes, noting that the tabulated t-value is 1.708 at the 0.05 level and 2.485 at the 0.01 level. This means that all t-values are highly significant and there are significant differences in the responses of the surveyed individuals for each question and for each axis of the questionnaire as a whole.

Fifth: Factor Analysis

The idea of factor analysis is based on studying the research sample's answers for each of the questionnaire's axes, then dividing the answers into groups according to the homogeneity of the values of those groups, so that each group consists of a number of variables (questionnaire questions), and at the same time showing the nature of the relationship of each variable with its group. The relationship may be negative, i.e., with an inverse effect, or positive, i.e., with a direct effect. To show the effect of this analysis on arranging the variables according to their importance from the point of view of the research sample's answers, we take the first axis, cybersecurity, as a model for this analysis from the point of view of the research sample.

Table (6) shows that this analysis of the research sample's responses to the cybersecurity axis consists of three groups whose total value ranged between 3.243 for the first group and 1.370 for the third group, with cumulative percentages ranging between 32.431% for the first group and 60.994% for the third group, and a variance percentage of 32.431 for the first group and 13.703 for the third group.

Table (6) shows the sequence of groups according to their values and the cumulative percentages of variance for each of them

Group sequence	**Total values for each group**	**Ratio of variance of the first group to the total**	**Cumulative ratios of group variance**
1	**3.243**	**32.431**	**32.431**
2	**1.486**	**14.860**	**47.291**
3	**1.370**	**13.703**	**60.994**

Table (7) shows the variables of the first axis ranked according to the degree of saturation of each variable, i.e., according to the degree of correlation of the variable with the group. This analysis ranks the importance of the questions in this axis from the perspective of the research sample's responses, not according to their order in the questionnaire.

Table (7) shows the degree of saturation of the variables (questionnaire questions) that have the greatest impact on the first axis, cybersecurity, from the perspective of the research sample, not as they are ranked in the questionnaire.

Question number according to the questionnaire	First axis variables: Cybersecurity	Saturation level
7	**Is the accounting data backed up daily, weekly, or monthly?**	**0.828**
6	**Is accounting data encrypted during transmission and storage?**	**0.748**
10	**How does weak cybersecurity affect the accuracy of financial reports?**	**0.666**
8	**What are the main threats facing digital accounting data in your business?** **- Cyberattacks** **- Malware** **- Internal data leaks** **- Human error**	**0.622**
2	**Do you have a grasp of the cybersecurity techniques applied in digital accounting?**	**0.599**
4	**Are strong, regularly changed passwords used to access digital accounting files?**	**0.511**

Table (8) shows that this analysis showed us that the research sample's answers to the cybersecurity axis consisted of four groups whose total value ranged between 3.271 for the first group and 1.037 for the fourth group, with cumulative percentages ranging between 29.736% for the first group and 67.106% for the fourth group, and a variance percentage of 29.736 for the first group and 9.423 for the fourth group.

Table (8) shows the sequence of groups according to their values and the cumulative percentages of variance for each of them

Group sequence	Total values for each group	Ratio of variance of the first group to the total	Cumulative ratios of group variance
1	**3.271**	**29.736**	**29.736**
2	**1.740**	**15.821**	**45.556**
3	**1.334**	**12.126**	**57.682**
4	**1.037**	**9.423**	**67.106**

Table (9) shows the variables of the second axis arranged according to the degree of saturation for each variable, i.e., according to the degree of correlation of the variable with the group. That is, this analysis ranks the importance of the questions of this axis from the point of view of the research sample's responses and not based on their order in the questionnaire.

Table (9) shows the degree of saturation of the variables (questionnaire questions) that have the greatest impact on the second axis, digital accounting, from the point of view of the research sample and not as they are arranged in the questionnaire.

Question number according to the questionnaire	Second axis variables: Digital accounting	Saturation level
10	Does a lack of technical expertise hinder the shift towards digital accounting?	**0.721**
7	Are the procedures for controlling access to accounting data dual?	**0.669**
3	Does digital accounting differ fundamentally from traditional accounting?	**0.615**
2	Do you have any idea about the technologies and tools used in digital accounting (e.g., systems, cloud, electronic signature)?	**0.605**
8	Does senior management encourage the shift to digital accounting?	**0.553**
5	Does digital accounting speed up financial reporting and reduce accounting errors?	**0.542**
9	Are there the necessary infrastructures, including personnel, equipment, and software, for digital accounting?	**0.538**

CONCLUSIONS

1. The shift to digital accounting is inevitable and aligns with the prevailing technological advancements worldwide. The transition from traditional to digital accounting is simply a matter of time.
2. Digital accounting requires a robust infrastructure, including human resources, equipment, electronic devices, and a comprehensive transition plan. If economic units develop plans and prepare the necessary equipment, the transition will be faster. If they fail to do so, the transition will still occur, but at a slower pace.
3. It is essential for economic units to adopt appropriate technologies that suit their operations and facilitate the transition to digital accounting. They must also train their staff and define their short- and long-term strategies.
4. The digital transformation in accounting must be accompanied by improvements in internal control methods and electronic protection of sensitive financial data related to economic units' accounts and customer balances.
5. The threats facing monetary data are serious and global, necessitating highly reliable tools and technologies to protect financial and monetary data. Failure to do so will transform the situation into a problem threatening economic and social security.

RECOMMENDATIONS

1. The transition from traditional to digital accounting requires implementing data protection measures against theft, manipulation, and fraud. Cybersecurity is paramount among these technologies.
2. Cybersecurity and electronic internal control technologies form the backbone of protecting financial and monetary data. Without them, the transition to digital accounting is impossible, as the risk level is high, reaching up to 100%.
3. Economic entities should train their staff to defend their financial data using global best practices. This necessitates the direct and continuous updating of technologies used to protect financial data and account balances.
4. It is possible to develop local systems for protecting accounting data, in addition to global cybersecurity technologies, to provide customers with confidence in the ability of economic entities to protect themselves and their clients from various types of hacker attacks. 5. The state, and not just economic units, should be responsible for developing cybersecurity technologies, because the issue is not related to the economic dimension, but rather to national security. Therefore, it requires expanding cybersecurity studies, creating solid postgraduate studies in this field, and developing a well-thought-out plan at the national level to improve the reality of cybersecurity.

Disclaimer (Artificial intelligence)

Dr. Naji Shayeb Al-Rikabi hereby declares that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

REFERENCES

1. Kuntoro, A., & Politeknik, YkPN, (2025) The role of digital accounting in transforming corporate finance in modern Era, Vol. 2 No. 3 (2025): The Journal of Academic Science . Indonesia.
2. Ali, S., & Hassan, M. (2021), The Evolution of digital Accounting: from Manual Bookkeeping to Cloud –Based Systems, International Journal of Accounting and Information Management.
3. Hassan, A., (2025), Implications of Digitalization on the Accounting Profession, Auditing Practices, and Accounting Education in Iraq: Challenges and Proposed Solution. University of Thi -Qar Journal, Vol.20 No. 3 September.

4. Zebua W., (2025), the role of Digital Transformation in Accounting System for the Transparency and Accountability of MAME Financial Statements. University Pancasila, Indonesia.
5. Alvina Y., Sridayanti W., Azzahra N.,(2024) Analysis of Block Chain Technology in Cybersecurity in the field of Accounting Systematic Literature Review. Vol. 16 No. 1 (2024): Journal Riset, Akuntansi, Indonesia.
6. Aisyah P. N., & Tjandrakirana R., (2025). Artificial Intelligence and cloud – Based Accounting Information Systems: Enhancing Financial reporting reliability and Cybersecurity in the digital Era, Vol. 4 No. 3: August 2025, University Sriwijaya, Indonesia.
7. Hasan L., Hossain M. Z., Johora F.T., Hasan M. H., (2024) Cybersecurity in Accounting: Protecting Financial Data in the Digital Age, European Journal of Applied Science Engineering and Technology.
8. Abu-Dabaseh F., Khtatbeh M. M., Alararah K., Alassuli A.(2025)
9. Exploring the role of digital transformation in Mitigating accounting fraud: A Cybersecurity perspective. International Review of Management and Marketing, 2025, 15(3), 398-405
10. Shchyrba I., Lagovska O.,Demianyshyna O., Myronchuk Z., Shebeshten E., (2024), Regulatory Challenges and Cybersecurity Approaches in Cloud Based Accounting Systems. Journal of Information Systems Engineering and Management, Vol. 10 No. 2s (2025)
11. Hazzaa L. H., Khanchel I.,) 2025), the Impact of Digital Transformation on the Security of Electronic Accounting Information Systems: A Survey of Iraq Banks.