Indonesian Journal of Law and Economics Review

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Indonesian Journal of Law and Economics Review

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Table Of Contents

Indonesian Journal of Law and Economics Review
Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Originality Statement

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

Conflict of Interest Statement

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

Copyright Statement

Indonesian Journal of Law and Economics Review

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

EDITORIAL TEAM

Indonesian Journal of Law and Economics Review

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

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

Indonesian Journal of Law and Economics Review

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Digital Transformation and its Role in Enhancing the Security of Accounting Information An Analytical Study of the Opinions of a Sample of Accountants from Private Banks in Baghdad Governorate: Transformasi Digital dan Perannya dalam Meningkatkan Keamanan Informasi Akuntansi: Studi Analitis terhadap Pendapat Sebagian Akuntan dari Bank Swasta di Provinsi Baghdad

Lecturer.Dr. Jasim Mohammed Yaseen, jasim.mohamad65@yahoo.com (*)
Al-Turath University , Baghdad, Iraq

Alaa Abd Al-hussen Omran Al-Zubaidi , alaaommran@yahoo.com
Al-Turath University , Baghdad, Iraq

Prof. Dr. Hikmat A. Alrawi, Hikmatalrawi12@yahoo.com
Al-Turath University , Baghdad, Iraq

(*) Corresponding author

Abstract

General Background Digital transformation has become a central theme in modern organizations seeking to adapt to technological advancements and evolving operational environments. **Specific Background** This study focuses on the integration of digital transformation practices within organizational and financial systems, particularly in relation to performance and information security. **Knowledge Gap** Despite growing attention, limited clarity exists regarding how digital transformation interacts with organizational processes and performance outcomes in specific institutional contexts. **Aims** The study aims to examine the role of digital transformation in shaping organizationalperformanceandsupportingsecureinformationsystems. **Results** Thefindingsindicate that digital transformation is associated with improved organizational processes, better data management, and stronger alignment with strategic objectives. **Novelty** The study offers a comprehensive perspective by linking digital transformation with both performance and information security considerations within organizations. **Implications** The results suggest that institutions should adopt structured digital strategies to optimize operational processes and ensure information security in dynamic environments.

Keywords: Digital Transformation, Organizational Performance, Information Systems, Strategic Management, Information Security

Key Findings Highlights

Integration of technology supports structured operational processes
Data management practices align with organizational objectives
Security considerations are embedded within transformation strategies

Published date: 2026-04-19

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Introduction

The world is going through a big transformation as it moves toward full digitization. Digital transformation is now a strategic necessity for using technology across all facets of an institution's operations to maintain a competitive edge and ensure company continuity amid fast change. Ismail (2022) believes that this transformation is "the process of companies moving towards business models that rely on digital technologies to innovate products and provide marketing channels that increase the value of their outputs." This implies that banks need to build flexible plans that use both cutting-edge leadership and cutting-edge infrastructure to save money and keep things running smoothly [1].

"Accounting information security" must be a major priority during this change to keep financial data safe from hacking and other threats. Khamis (2021) believes that we need to "make big changes to the way we work to better and faster serve beneficiaries." It doesn't only mean changing records into digital files; it also requires building a digital control system that makes sure processing is done well and accounting outputs are right in a paperless environment [2]. Slimi and Bushi (2019) argue that IDC's idea of digital transformation is "an ongoing process of adapting to market demands by leveraging digital capabilities to create business models that seamlessly blend digital and manual operations." This study aims to investigate the influence of the dimensions of digital transformation—strategy, culture, and leadership—on the improvement of accounting information security in private banks in Baghdad, with the objective of creating a robust banking environment that protects its information assets and guarantees financial stability in a dynamic technological context [3].

In this context, the researcher delineated the problem of the current study by examining previous research and suggesting a framework of terms that clarify the relationship between the two variables under investigation: digital transformation and accounting information security. This study has prompted numerous inquiries concerning the nature of the association between the study variables inside private banks in the Baghdad Governorate. In response to these inquiries, the current study delineated certain objectives, which it seeks to achieve by the application of a particular collection of data and facts, and to determine the nature of the relationship among the components being examined. The statistical analysis facilitated the current study in drawing conclusions that clarify the relationship among the examined variables and in developing a set of recommendations.

1- Methodology of the study.

1-1- Research problem:

The research problem lies in the growing gap between the accelerating trend of private banks towards digital transformation and the complex security challenges facing accounting systems. Theoretically, there is a need for a conceptual framework that links the dimensions of digital transformation to mechanisms for enhancing the security of accounting information in paperless environments. Practically, the problem stems from the varying levels of leadership and organizational culture responsiveness to the cyber risks threatening the financial data of banks in Baghdad. This could weaken the effectiveness of internal control systems and threaten the reliability of accounting reports for stakeholders. Therefore, it is necessary to determine the extent to which the adopted digital strategies contribute to safeguarding this information and ensuring its continuity.

Based on the research problem we have formulated (theoretical and applied) and the preceding introduction, the main research question can be formulated in a precise scientific manner that combines the independent and dependent variables of the study as follows:

"What is the role of the dimensions of digital transformation (digital strategy, digital organizational culture, and digital leadership) in enhancing the security of accounting information in private banks operating in Baghdad Governorate, and to what extent are these dimensions effective in mitigating the technical risks facing accounting systems from the perspective of a sample of accountants?"

1-2- Importance of the study:

The theoretical significance of the research is manifested in its enhancement of the accounting and administrative library by offering a contemporary intellectual framework that integrates the philosophy of digital transformation with the security of accounting information, thereby addressing the knowledge deficit regarding the protection of financial systems within the Iraqi business context. In terms of practical importance, it is emphasized by giving decision-makers in private banks in Baghdad a guide on how to use the dimensions of digital transformation to improve the quality of internal control and keep data safe from breaches. This builds trust and credibility in banking financial reports and helps these institutions deal with quickly changing cyber threats with high efficiency.

1-3- Study Objectives:

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

- To determine the level of digital transformation (digital organizational culture, digital strategy, and digital leadership) from the perspective of accountants in private banks in Baghdad Governorate.
- To measure the level of accounting information security from the perspective of accountants in private banks in Baghdad Governorate.
- To analyze the relationship between digital transformation and accounting information security from the perspective of accountants in private banks in Baghdad Governorate.
- To provide practical recommendations to private banks in Baghdad Governorate to enhance accounting information security through digital transformation.

1-4- Study Hypotheses

Based on the theoretical assumptions that will address the study variables (digital transformation and accounting information security), and in order to achieve the objectives and answer the research questions, the following hypotheses were developed:

Main Hypothesis: There is no statistically significant relationship between digital transformation and enhancing accounting information security. From this main hypothesis, the following sub-hypotheses emerge:

- Sub-hypothesis 1: There is no statistically significant relationship between digital strategy and enhancing accounting information security.

- Sub-hypothesis 2: There is no statistically significant relationship between digital organizational culture and enhancing accounting information security.

- Sub-hypothesis 3: There is no statistically significant relationship between digital leadership and enhancing accounting information security.

1-5- The study's hypothetical framework:

"Based on the study's problem, its importance, and its objectives, the study's hypothetical framework was designed. This framework illustrates the relationships between the study variables: digital transformation as the independent variable, represented by two paths (digital strategy, digital organizational culture, and digital leadership), and accounting information security as the dependent variable. Figure (1) illustrates the study's hypothetical framework".

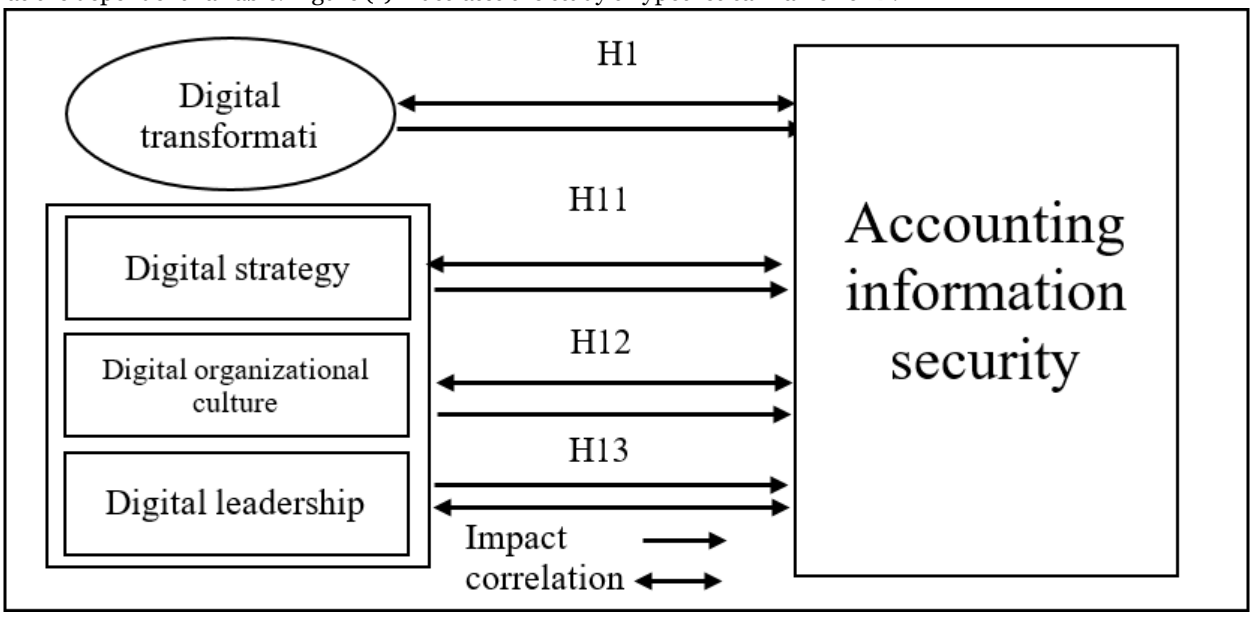

Figure ( ) The hypothetical model of the study
Prepared by the researcher based on the literature

1-6- Methodology and approach of the study

The researcher employed the descriptive analytical method to complete the theoretical and field frameworks of the study. This method aims for precision in identifying the problem, followed by analysis to uncover the influencing relationships among its variables, facilitating interpretation and conclusions that aid in diagnosing the reality, while aligning with the scientific method and the study's objectives.

1-7- A description of the study population and sample

Indonesian Journal of Law and Economics Review
Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

One of the most important things that makes sure the results are accurate and true and that the study hypotheses are tested is choosing the right study location and population. Consequently, a selection of commercial banks examined in Baghdad Governorate will be made (Gulf Commercial Bank, National Islamic Bank, Middle East Iraqi Investment Bank, Regional Commercial Bank, Al Rajhi Islamic Bank). Nonetheless, not all employees are directly associated with the study variables and objectives. Consequently, the researcher may choose a target subgroup, which Saunders et al. (2016, p. 275) refer to as a subgroup of the population known as the target population. The researcher delineated the target group as accountants employed solely by the aforementioned banks, as they represent the most appropriate subjects for the study variables, totaling 275 accountants [4].
In order to determine the appropriate sample size, the following equation was used, which was mentioned by (Steven K. Thompson, 2012) for determining the sample size [5],

$$n = \frac{N \times p(1-p)}{\left[\left[N-1 \times \left(d^2 \div z^2\right)\right] + p(1-p)\right]}$$

N=	Population size
z=	Standard score corresponding to a significance level of 0.95 equals 1.96
d=	Percentage of error equals 5%
P=	Availability and neutrality ratio = 0.50

This suggested that a minimum of sixteen hundred and sixty-one accountants would be an ideal sample size. Hence, a random sample was given 170 questionnaires. After 166 questionnaires were returned, it was determined that a total of 164 questionnaires were valid for statistical analysis. This is more than the required number to accurately represent the community.

The demographic data for the study sample included four (4) elements as control variables to measure their degree of influence on the dependent variable, in addition to the influence of the independent variable. The dependent variables are: gender, educational qualification, age, and years of work experience, as shown in the table below.

Table (1) Analysis of the Demographic Data for the Study Sample*

Description	Category	repetition	%
Gender	Males	**112**	**68.3%**
	Females	**52**	**31.7%**
Age Group	25-35	**25**	**15.2%**
	36-45	**48**	**29.3%**
	46-55	**63**	**38.4%**
	56 and above	**28**	**17.1%**
Certification	Diploma	**18**	**11.0%**
	Bachelor's	**87**	**%53.0**
	Master's	**32**	**19.5%**
	PhD	**27**	**16.5%**
Years of Experience	Less than 5 years	**31**	**%18.9**
	5-10 years	**58**	**35.4%**
	11-15 years	**43**	**26.2%**
	16 years and above	**32**	**19.5%**
the total		**164**	**%100.0**

"Source: Prepared by the researcher based on data from the field study" (2026).
The table above shows the following:

1. Gender Variable: The male category had the highest value, with a frequency of 112 and a percentage of 68.3%. The female category had the lowest value, with a frequency of 52 and a percentage of 31.7%. This shows what the private banking sector's workforce is like. Men are more likely to be in these jobs.
2. Age Variable: Most of the sample groups are in the professional maturity stage. The 46-55 age group had the highest value at 38.4%, while the 25-35 age group had the lowest value at 15.2%. This shows that private banks depend on skilled workers to handle accounting and security data.
3. Educational Attainment Variable: The bachelor's degree made up the most part of the sample's academic descriptors, with 87 instances and 53.0% of the total. The diploma category had the lowest value, at 11.0%. This shows that the banks are serious about hiring college graduates with the right skills for the challenges of digital transformation and information security.
4. Years of experience variable: The data shows that the cumulative experience is good, with the (5-10 years) experience category having the highest value at 35.4% and the (less than 5 years) experience category having the lowest value at 18.9%.

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

This means that the sample responses are very reliable because they are from the same time period as the stages of technological development in the banking system.

1-8- Checking to see if the study instrument is valid

A measurement instrument's validity is its capacity to accurately measure what it was meant to measure. The notion of proper measurement says that perfect validity means that the instrument has no measurement mistakes at all, whether they are random or systematic. The study used the following standards to make sure that the measurement tool was valid:

Second, Instrument Reliability: The validity of an instrument shows how well it can measure what it is supposed to measure, including how well it covers all the relevant parts and how clear its items are. To guarantee this, the researcher executed a pilot study with 40 questionnaires, employing Cronbach's alpha to assess the internal consistency of the data. Cronbach's alpha can be anywhere from 0 to 1, and the closer the value is to 1, the more consistent the results are. Some sources, like Hair et al. (2010), say that a value higher than 0.70 is better, but Bowling (2009) and Nonnally (1967) say that values of 0.50 and higher are appropriate during the early stages of fundamental research [6].

The pilot sample's Cronbach's alpha test findings are shown in Table (2).

Independent and dependent variables	Components of the variables	**Number of paragraphs**	**Cronbach's alpha coefficient value**	**Validity coefficient value**
digital transformation	Digital strategy	5	%87.7	93.6%
	Digital organizational culture	5	%90.4	95.1%
	Digital leadership	5	%89.2	94.4%
Accounting Information Security		10	%87.9	93.8%
Questionnaire		25	%88.8	94.2%

"The researcher used SPSS software to make the source."
"The table above shows that they all fell within acceptable limits".

1-9- Study Limitations

The study limitations are as follows:

- Knowledge Limitations: The study's knowledge limits are defined by the main variables, namely (digital transformation and accounting information security) and their sub-dimensions.
- Time Limitations: The study's time limit is the year 2026.
- Spatial Limitations: The spatial limitation is defined by the research field chosen to test the study's hypotheses and answer its questions. This field is defined as (private banks in Baghdad Governorate), namely (Gulf Commercial Bank, National Islamic Bank, Middle East Iraqi Investment Bank, Regional Commercial Bank, and Al Rajhi Islamic Bank).
- Human Limitations: The study's human limitation is defined by the accountants of the commercial banks studied in Baghdad.

2- Theoretical Framework

2-1- The Concept of Digital Transformation

A paradigm shift is also essential for the successful implementation of digital technologies across all aspects of organizational operations. To achieve this, one needs to cultivate a digital culture that emphasizes agility, innovation, and collaboration. A culture deeply rooted in digital practices can help companies adapt quickly to changing market conditions, adopt emerging technologies, and foster a lifelong learning and development mindset.

Ismail (2022) defined digital transformation as "the process by which companies move to business models based on digital technologies to support the development and innovation of their products and services, and to provide new marketing channels and job opportunities that increase the value of their products, whether goods or services [1]." Khamis (2021: 18) defined it as the change associated with the application of digital technology to bring about a radical change in the way they work and to serve

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

beneficiaries faster and better [2]. IDC defined digital transformation as "the continuous process by which organizations adapt to the requirements of their customers and markets (the external ecosystem) by employing digital capabilities to create new business models, products, and services that seamlessly blend digital and manual work and customer experiences while simultaneously improving operational efficiency and organizational performance" [3]. Therefore, digital transformation does not simply mean shifting towards the use of technology within the company's boundaries, but is a comprehensive program that encompasses the entire company, fundamentally in terms of internal and external work methods and in terms of providing services to the target audience to deliver services easily and quickly. Consequently, digital transformation drives companies to change their models. Its operations and adaptation to the new market reality [1].

2-2- Objectives of Digital Transformation.

Digital transformation ensures several objectives that companies strive to achieve by generating value through digital ideas and innovations, and by presenting business models in a new way using the fastest and most innovative technologies. This leads to significant speed and growth for the company [7]. Ebert & Duarte (2018:16) identified a set of objectives, which are as follows [8]:

- Promoting and developing a more creative and collaborative culture within the company and society.
- Transforming the education system to provide new skills and future-oriented guidance for employees so they can achieve excellence in digital work and society.
- Establishing and maintaining digital communication infrastructure and ensuring its management, accessibility, service quality, and affordability.
- Enhancing digital data protection, transparency, independence, and trust.
- Improving accessibility and the quality of digital services provided.
- Implementing new and innovative business models to achieve the goal.
- Working to implement innovative practices and improve the regulatory framework and technical standards.

2-3- Aspects of Digital Transformation.

Digital transformation has many parts, such as:

3-2-1- The Idea of a Digital Strategy

Digital strategy is the main thing that people in an organization use to bring their ambitions and efforts together. It serves as a focus point, curtailing the dispersion of efforts and steering them directly towards the attainment of specified digital objectives [9].

In terms of operations, it is the set of administrative decisions and processes that the organization uses to reach its quality goals. This strategy is responsible for shaping the organization's future and formulating its operational standards, in accordance with the nature of its activity and the competitive tactics it employs in the face of its market counterparts [10].

3-2-2- The Idea of Digital Organizational Culture

Digital organizational culture is the set of values and beliefs that everyone in the organization shares. It operates as a dynamic system that interacts adaptively with human resources, organizational structures, and the internal control systems of the organization [11].

In a similar vein, it is an enduring and universally applicable institutional phenomena, manifested through ongoing social interactions. It is a social model based on common core beliefs that members of the organization come up with to figure out how to deal with problems and adapt to the outside world and integrate with the inside world in the digital age [12].

3-2-3- The Idea of Digital Leadership

Digital leadership is a new idea in management that has come out recently. It is mostly about finding a balance between the need for stability in an organization and the fact that digital transformation is going to happen. Digital leaders are the ones that boost morale and instill values in their employees, which makes them think about how to come up with new ways to solve operational challenges [11]. This kind of leadership needs a lot of flexibility to deal with the changing digital world, which means that the organization has to make sure that its internal circumstances are in line with these outside forces [13].

Researchers assert that the efficacy of digital leadership is contingent upon its capacity to elevate employee performance standards, as delineated by Bass (1995) [14]. This entails enhancing individuals' personal values and self-concept to align with elevated levels of professional ambition (Cheung, 2011: 659). These leadership techniques have a direct effect on all of the

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

organization's administrative tasks and general activities (Al-Sudani, 2014: 38). Even if there are many different views on what digital leadership is and how to define its goals, it is still the most important thing for creating digital trends in modern businesses.

2-4- The concept of information security

Information security is the process of safeguarding information from risks that threaten or attack it by implementing a set of procedures and preventive measures that are employed in the technical or preventive field to preserve information, devices, and software, as well as procedures that are related to the preservation of workers in this field [15]. It is a collection of preventive measures that are employed in the administrative and technical sectors to safeguard data resources, including devices, software, and data, from violations or illegal interventions that may occur by chance, intentional sequence, or incorrect procedures used by information resource management. Additionally, it includes procedures to address the risks associated with potential natural disasters that may result in the loss of some resources in whole or in part, thereby affecting the quality and level of service provided [16]. Information security is also the field of science that investigates the theories, strategies, and laws that safeguard information from potential hazards. It entails the implementation of the requisite methods, procedures, and means to ensure this protection, confront and surmount risks, and enact strict laws to prevent future occurrences and punish perpetrators. The application of information security from all scientific, practical, and legal perspectives has a substantial effect on the enhancement of confidence in accounting information systems [17].
It is also defined as the examination of policies and strategies that must be comprehended in order to safeguard information from a variety of threats and attacks [18].

2-5- Elements of Information Security

To protect information from exposure risks, a series of elements must be provided to ensure adequate protection. These elements are divided into [19]:

- **Reliability or Confidentiality:** This means that unauthorized individuals cannot view or disclose the information.

  To achieve this, organizations must employ appropriate security measures in various ways, such as message encryption or preventing the identification of the size or path of the information transmitted.

- **Personal Identity Verification**: This means confirming the identity of the person attempting to use the information and determining if they are the correct user. This is illustrated by the use of a password for each user. There are three methods of identity verification [20]:
  a. Things the person knows, such as passwords.
  b. Things they possess (e.g., a token), which is a code the user enters into the computer to obtain authorization or an electronic certificate.
  c. By the person's physical characteristics, such as fingerprints, network scans, or voice recognition. Each method has its advantages and disadvantages.

- **Content Integrity:** This refers to ensuring the accuracy of the information content and that it will not be altered, corrupted, or tampered with at any stage of processing or exchange, whether the transaction is conducted internally or externally by an unauthorized person. Such incidents are usually the result of illegal intrusions, such as viruses. For example, no one can corrupt a bank's database and change the account balance. Therefore, the organization is responsible for ensuring content security by taking appropriate preventative measures, such as software, antivirus, anti-hacking, or antivirus hardware.

- **Service or information availability:** This refers to ensuring the continuity of the information system's functions and all its components, as well as the continuous ability to interact with information and provide services to information sites, and ensuring that information users are not exposed to the information they are at. It also involves preventing its illegal use or unauthorized access. Alternatively, it can refer to a method by individuals to disrupt an organization's services through a large number of unsolicited emails on the network [21].

- **Non-repudiation:** This means ensuring that a person performing a specific action related to information cannot deny this action. Therefore, there must be a way or means to prove any action taken by anyone against the person performing the action. For example, at a specific time, to ensure that goods purchased online reach their owner and to prove that the transfer was an electronic payment, various methods such as electronic signatures and electronic identity verification can be used.

3- The Research's Practical Framework

3-1- Descriptive Statistics of the Study Variables

Indonesian Journal of Law and Economics Review
Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

We found the standard deviation and mean for each statement and axis in order to look at the study data. The arithmetic mean being higher than the hypothetical mean of 3 showed that people agreed on the items. The table below illustrates the means, standard deviations, and how important each assertion in the study is. In general, standard deviations that are near to 1 show that the answers of the people in the sample are very similar. Moreover, all mathematical means surpassed the hypothetical mean, so affirming the substantial consensus about all claims of the study variables.

3-1-1- A description of the digital transformation variable through analysis

The numbers in the table show that the banks surveyed usually had a good opinion of the different aspects of digital transformation. The entire variable had an average of 3.48, which was greater than the imagined average of 3. It had an agreement rate of 69.6% and a standard deviation of 0.751. This shows that the people in the survey sample believe that digital transformation is important and that there is a real trend toward using new technology to improve banking operations and information security.

- About the digital strategy: The digital strategy got a lot of responses, with a mean of 3.52 and a 70.4% agreement rate. The second question, which was about how well the transformation approach fit with the bank's goal, came in first with a score of 3.65. This shows that private banks in Baghdad have a clear strategic vision for how to use technology to help the institution reach its goals and make sure that the digital transformation goes smoothly and as planned.
- Digital Organizational Culture: The results showed a clear interest in creating a digital culture, with a mean score of 3.51. The highest score in this area was 3.76 for item 8, which was about how well employees fit into operational functions. This shows that banks are working to make the workplace more collaborative and use technology in their everyday tasks. However, they still need to improve the skills and talents they need to stay up with fast changes.
- Digital Leadership: The digital leadership dimension had a mean score of 3.41 and a percentage of agreement of 68.2%. The item about how employees can help drive the transformation vision came in first with a mean score of 3.63. This shows how important leadership is in getting people to work hard and think creatively, which helps reduce opposition to digital change and make sure that security and accounting regulations are followed correctly.

Table No. (3) Means and Standard Deviations for the Digital Transformation Variable

	Paragraphs At our bank, the following is disclosed:	arithmetic mean	standard deviation	Agreement %	C.V	NO.
.1	The bank must establish a clear and written vision and mission for the digital transformation process.	3.46	0.777	69.2%	22.5 %	4
.2	There must be consistency between the digital transformation strategy and the bank's vision, mission, and objectives.	3.65	0.654	73.0%	17.9%	1
.3	The bank must develop a strategic direction for a complete transition to digital transformation.	3.61	0.678	72.2%	18.8%	2
.4	The bank's policies must be adapted to implement the desired digital transformation strategic plan.	3.33	0.874	66.6%	26.2 %	5
.5	The bank's strategy must be periodically reassessed to ensure alignment with the digital transformation process.	3.56	0.711	71.2%	20.0 %	3
	Digital Strategy	3.52	0.739	70.4%	21.0%	
.6	The bank is committed to expanding employee participation in the digital transformation process.	3.66	0.645	73.2%	17.6%	2
.7	The bank is committed to expanding employee participation in the digital transformation process.	3.21	0.869	64.2%	27.1%	5
.8	The bank integrates employees in operational roles into the digital transformation process.	3.76	0.598	75.2%	15.9%	1
.9	The bank provides the necessary modern technologies to develop the systems and services offered to beneficiaries.	3.41	0.793	68.2%	23.3 %	4
10	The bank is committed to improving the level of services provided.	3.53	0.724	70.6%	20.5 %	3
	Digital Organizational Culture	3.51	0.726	70.3%	20.7 %	
11	The bank engages employees in driving the digital transformation vision.	3.63	0.604	72.6%	16.6%	1
12	The management motivates employees to achieve the vision and objectives of the	3.11	0.908	62.2%	29.2 %	5

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

	digital transformation process.					
13	The bank's senior management encourages intellectual stimulation from employees, fostering openness to new ideas and problem-solving.	3.52	0.784	70.4%	22.3 %	2
14	The bank prioritizes aligning employee capabilities with the digital transformation process.	3.43	0.808	68.6%	23.6 %	3
15	The bank empowers employees to achieve optimal performance.	3.35	0.838	67.0%	25.0 %	4
Digital Leadership		3.41	0.788	68.2%	23.1%	
	Total Digital Transformation	3.48	0.751	69.6%	21.6%	

"The researcher used SPSS software to make the source."

3-1-2- A descriptive analysis of the variable for accounting information security

The statistical results for the accounting information security variable demonstrate a substantial positive reaction from the sample. The overall mean is 3.53, which is much higher than the hypothetical mean, and the overall agreement rate is 70.5%. This shows that accountants at private banks in Baghdad are very aware of the rules for digital security. Item 10, which was about improving staff productivity through training courses, came in first with a mean of 3.83. Item 5, which was about the distribution of specializations, came in second with a mean of 3.74. The question about protecting electronic signatures, item 4, got the fewest responses, with a mean of 3.19. The low coefficient of variance of 21.0% shows that the surveyed banks had quite different views on this issue. This shows that they see human resources and administrative control as the first line of defense for protecting accounting data. But in the future, we need to work on making electronic signature protection and encryption technologies better to make the digital security system comprehensive.

Table No. (4) Means and Standard Deviations for the Accounting Information Security Variable

	Paragraphs	arithmetic mean	standard deviation	Agreement %	C.V	NO.
1.	The bank has an integrated information security system.	3.68	0.658	73.6%	17.9%	3
2.	The bank has an encryption and coding system for data and information.	3.48	0.803	69.6%	23.1%	7
3.	An internal control system is necessary to protect the transfer of electronic documents.	3.59	0.723	71.8%	20.1%	5
4.	Oversight is necessary to protect electronic signatures within the bank.	3.19	0.904	63.8%	28.3%	10
5.	Supervision and responsibilities are distributed among the staff at the computer center.	3.74	0.621	74.8%	16.6%	2
6.	Bank employees are involved in password management.	3.21	0.865	64.2%	26.9%	9
7.	There is a malfunction in the computers used when implementing the system.	3.51	0.768	70.2%	21.9%	6
8.	The staff responsible for implementing the system lack the necessary academic qualifications and practical experience to apply the electronic system.	3.63	0.701	72.6%	19.3%	4
9.	The electronic programs are not subject to continuous updates and development.	3.39	0.824	67.8%	24.3%	8
10.	Increase employee efficiency by enrolling them in training courses on using the electronic accounting information system.	3.83	0.528	76.6%	13.8%	1
Total accounting information security		3.53	0.740	70.5%	21.0%	

"The researcher used SPSS software to make the source."

3-2- Confirmatory Factor Analysis

Indonesian Journal of Law and Economics Review
Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

Confirmatory factor analysis (CFA), a type of structural equation modeling (SEM), was used to check that the factor constructions for the research variables were correct. This approach facilitates the evaluation of the validity of certain measurement models derived from previous theoretical frameworks, in contrast to exploratory factor analysis. The study utilized the maximum likelihood method to estimate parameters with AMOS V26 software. The analysis checks how well the covariance matrix of the variables fits with the model's assumed matrix. It then gives several fit quality indices to see if the proposed model is a good fit for the data.

The primary criterion for evaluating a model in confirmatory factor analysis is the degree to which the actual covariance matrix of the variables aligns with the expected matrix of the model. This study generates various statistical indicators that demonstrate the quality of this fit. The values of these indicators determine whether the proposed model is approved or rejected. The table below demonstrates how well the structural research model fits by showing the indications.

Table No. (5) Conformity Quality Indicators for Digital Transformation

Goodness-of-fit Measures	Acceptable Level
Chi-squirex^2 =	Not statistically significant at 0.05
P Close	>0.05
Adjusted goodness of fit index (AGFI)	90≥
Tucker-Lewis Index (TLI)	90≥
Goodness of fit index (GFI)	90≥
Root-mean-squire error of approximation (RMSEA)	< 0.08
Normal fit index (NFI)	90≥
/dfx^2	$1 < x^2/df < 5$
Comparative fit index (CFI)	90≥

"The researcher used SPSS software to create the source." Based on (Hair et al. 2010) [6]

Table (6) Results of the standardized regression weights for the research variable

Paragraphs	Paths	Dimensions	Estimate	S.E.	C.R.	P
X11	<---	Digital strategy	.602	.065	8.611	***
X12	<---		.678	.076	9.787	***
X13	<---		.786	.080	11.490	***
X14	<---		.766			
X15	<---		.768	.081	11.204	***
X21	<---	Digital organizational culture	.694	.113	7.541	***
X22	<---		.840	.127	8.373	***
X23	<---		.829	.134	8.322	***
X24	<---		.554			
X25	<---		.448	.109	5.532	***
X31	<---	Digital leadership	.720	.080	12.147	***
X32	<---		.883	.062	16.685	***
X33	<---		.804	.068	14.316	***
X34	<---		.851	.063	15.683	***
X35	<---		.846			
Y1	<---	Accounting information security	.587			
Y2	<---		.770	.141	8.812	***
Y3	<---		.745	.141	8.622	***
Y4	<---		.847	.145	9.355	***
Y5	<---		.730	.133	8.506	***
Y6	<---		.642	.110	7.781	***
Y7	<---		.739	.130	8.576	***
Y8	<---		.726	.148	8.480	***
Y9	<---		.702	.145	8.283	***
Y10	<---		.801	.135	9.038	***

"Source: The researcher made this based on the results of the statistical package (AMOS.V.26)."

The table and figure below show that the model fit indices taken from the AMOS software show a good fit between the proposed model and the actual data. The weighted chi-squared value (CMIN/DF) was 3.490, which is acceptable (less than 5). The comparative and structured fit indices (CFI, TLI, and IFI) likewise had values between 0.963 and 0.969, which is higher than the desired value of 0.90. The RMSEA value of 0.072 was also less than 0.08, which further confirmed that the model fit the data well.

3-3- Impact Hypotheses

Indonesian Journal of Law and Economics Review
Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

To analyze the impact relationships between the variables in this study, Structural Equation Modeling (SEM) was used. AMOS V26 software (Afthanorhan et al., 2014) was used to calculate the direct effects between the study variables, namely digital transformation in digital repositories and accounting information security.

First: Hypothesis (H1): The main hypothesis states: "There is a statistically significant impact of digital transformation on enhancing accounting information security." In order to substantiate this hypothesis, a structural framework was developed to illustrate the structure of the relationship between digital transformation and accounting information security. The findings of the inference statistics concerning the relationship between digital transformation and enhancing accounting information security show that the standard regression weights recorded values of (S.R.W = 0.632). The value of (R^2) indicates that digital transformation explains (46%) of the changes that occur in accounting information security, while the remaining percentage of (54%) is attributed to elements outside the study model. The value of (t) obtained for (S.R.W) for the digital transformation variable was (8.432). This value exceeds the recorded value of t of 1.96, indicating the stability of the S.R.W. value. The S.R.W. value shows that a one-unit increase in digital transformation leads to a 63.2% increase in accounting information security. Therefore, the hypothesis can be accepted: there is a statistically significant effect between digital transformation and enhanced accounting information security.

Table (7) Regression Model between Digital Transformation and Accounting Information Security

	Independent variable	Standardized regression weights **S.R.W**	**(t)**	**R Square**	**Sig**
Accounting Information Security	Digital transformation	**0.632**	**8.432**	**0.46**	**0.000**
	(t) Tabular decision	**1.96**			
	Independent variable	**Accepting the hypothesis**			

"Source: The researcher made this based on the results of the statistical package (SPSS)."

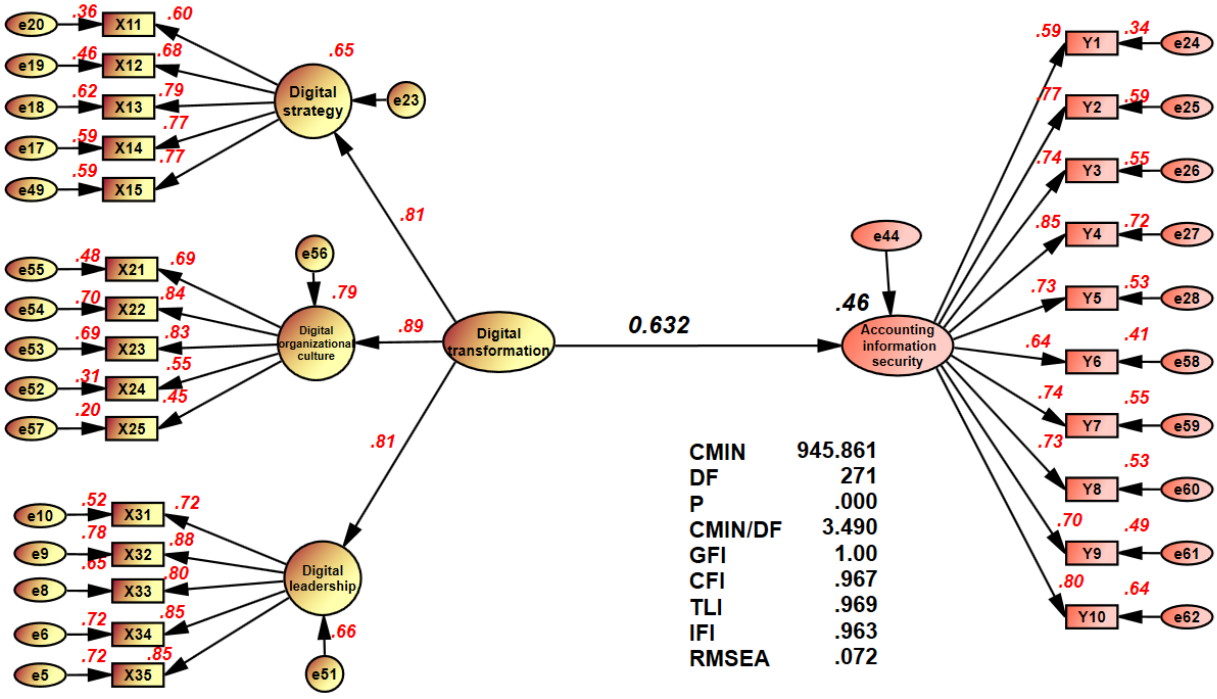

Figure (2) Impact Analysis of Digital Transformation in Accounting Information Security

"Source: Prepared by the researcher based on the outputs of the statistical package AMOS.V.26".

The following sub-hypotheses stem from the main hypothesis:

The following a multiple regression approach was employed to substantiate these hypotheses:

- **First Sub-Hypothesis (H1-1): The first sub-hypothesis states: ("There is a statistically significant effect" of the digital strategy in enhancing accounting information security.)**

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

The table below shows The findings of the inference statistics concerning the digital strategy in enhancing accounting information security. The standard regression weights recorded values of (S.R.W = 0.345). The model explains (26%) of the value of the variables occurring in the respondent variable, while the remaining percentage, amounting to (74%), is attributed to elements outside the study model. The t-value obtained for (S.R.W) for the digital strategy variable was (7.123). This value exceeds the recorded value of t of 1.96 indicates the stability of the S.R.W. value. This value shows that increasing the digital strategy by one unit leads to a 34.5% increase in accounting information security. Therefore, the hypothesis (that there is a statistically significant effect of digital strategy on enhancing accounting information security) can be accepted. It is clear that putting a strong emphasis on digital strategy, by using advanced technology policies that make sure data flows correctly and accounting systems are updated regularly, as well as providing strong control frameworks that limit access and usage permissions, directly helps to improve the security of accounting information and protect it from technical risks.

- **The second sub-hypothesis (H1-2) states: ("There is a statistically significant effect of digital organizational culture on enhancing accounting information security.")**

The table below shows The findings of the inference statistics concerning the relationship between digital organizational culture and enhancing accounting information security. The standard regression weights recorded values of (S.R.W = 0.256). The model explains 18% of the values of the variables occurring in the respondent variable, while the remaining 82% are attributed to elements outside the study model. The t-value obtained for the S.R.W. for the digital organizational culture variable was 7.456, This value exceeds the recorded value of t of 1.96. This indicates the stability of the S.R.W.'s significance. The S.R.W. value shows that increasing digital organizational culture by one unit leads to a 25.6% increase in accounting information security. Therefore, the hypothesis can be accepted: there is a statistically significant effect between digital organizational culture and enhancing accounting information security. The above shows that this is a big part of it. The studied banks need to pay more attention to digital organizational culture by getting employees involved in digital operational functions and teaching them how to handle data safely. They also need to create a technological work environment that makes it easy to access and clearly audit accounting information. Directly improves the security of accounting data by lowering the chance of human error and making internal control mechanisms work better.

- **Third Sub-Hypothesis (H1-3): It states: "There is a statistically significant effect of digital leadership in enhancing the security of accounting information."**

The table below shows The findings of the inference statistics concerning digital leadership's impact on enhancing the security of accounting information. The standard regression weights recorded values of (S.R.W = 0.176). The model explains (13%) of the values of the variables occurring in the respondent variable, while the remaining percentage, amounting to (87%), is attributed to elements outside the study model. The t-value obtained for (S.R.W) for the digital leadership variable was (7.654), This value exceeds the recorded value of t of 1.96. This indicates the consistent significance of (S.R.W). It is clear from the value of (S.R.W) that increasing digital leadership by one unit will lead to an increase in the security of accounting information. With a percentage of (17.6%), the above supports the hypothesis that (there is a statistically significant effect between digital leadership and enhancing accounting information security). The above shows that digital leadership is very important in the banks studied. This is because senior management has a clear technological vision that encourages employees to be creative and learn new things, while also giving them the support they need to improve digital control systems and keep access privileges private. The leaders' dedication to properly assigning technical duties and directly overseeing data protection systems helps improve the security of accounting information and make the banking environment strong enough to handle cyber threats with ease and speed.

Table (8) Analysis of the Impact of Digital Transformation Dimensions on Accounting Information Security

Index	**dependent variable**			
	Digital leadership	Digital organizational culture	Digital leadership	**Accounting Information Security**
(S.R.W)	**0.345**	**0.256**	**0.176**	
(R^2)	**0.26**	**0.18**	**0.13**	
(t)	**7.123**	**7.456**	**7.654**	
P	**0.000**	**0.000**	**0.000**	
(t) Tabular	1.96			
decision	Accepting the hypothesis	Accepting the hypothesis	**Accepting the hypothesis**	

Source: "SPSS program "

4- Recommendations and Conclusions

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

4-1- the conclusions:

1. The investigated private banks have a high level of adoption and implementation of digital transformation, which shows that their management believes that technology is important for improving banking operations. These banks have clear strategic plans that show this tendency. They want to make sure they stay up to date with changes in the global financial sector by incorporating new technologies into their core operations.
2. The results showed that accounting staff were quite aware of digital security requirements, with a strong focus on the human aspect as the first line of protection. The study finds that banks put a lot of effort into improving their workers' productivity and sharing supervisory duties, even though they need to focus on strictly technical issues like encryption systems and protecting electronic signatures.
3. The study showed that the digital strategy had a statistically significant positive effect on making accounting information more secure. This is because well-thought-out technical policies help protect financial data. A clear strategic vision and regular system updates provide a strong supervisory environment that limits access rights and lowers the danger of cyber attacks.
4. The results showed that a digital organizational culture is very important for information security since it lowers the chances of human error caused by a lack of technological knowledge. It concludes that fostering a collaborative workplace that promotes clear and transparent technology use improves the effectiveness of internal control systems and streamlines digital accounting audits.
5. The study found that digital leadership is the most important factor in the effectiveness of accounting security systems. This is because senior management took an innovative approach and gave the technical support that was needed. It finds that leaders' dedication to actively managing the allocation of technical duties and intellectually stimulating workers generates a resilient banking environment capable of adjusting successfully to emerging security issues.

4-2- Recommendations

A. Must evolve the digital strategy of private banks in accordance with international information security standards They must create an "accounting security policy" that is specific and feeds into their vision. This provides a legal and technical basis to keep financial data secure from future breaches.
B. Companies can also conduct continuous awareness programs from time to time enabling employees towards digital literacy that will help bring the gap of digital divide in a way. Finally, all accountants need to be educated about the potential for human error to undermine the accounting system and so it is vital that they understand how social engineering works and why they must maintain confidentiality over database information.
C. Enabling Digital Leadership by less on things and more on connecting Slalom, empowering technically gifted accountants to drive new thinking. The information technology must function with a proliferation of strong encryption systems and surveillance so that electronic access can be tracked in real-time and around the clock, to avoid repeating mistakes from years gone past. D. Provide specialized training in courses like "Accounting Information Security" and electronic auditing. And connect employees' digital and security skills to their career paths and promotion prospects. This will ensure their swift and efficient deployment of vital technologies.
D. Adopt electronic signature and encryption technologies, and keep your accounting software up to date. In addition, to ensure the accuracy and tamper-proof nature of financial reports in the paperless digital world, create real-time electronic internal control system that automatically checks and audits accounts.

Reference

1. A. F. Bouarar, R. E. Fattah, and R. Ismail, "The Contribution of Intellectual Capital to Achieving Digital Transformation to Improve Social Services for Elderly People with Disabilities," Journal of Faculty of Social Work and Social Studies Research, vol. 27, no. 2, pp. 215–260, 2022.
2. A. Khamis and Aser, "The Impact of Digital Transformation on the Job Performance of Employees in Egyptian Commercial Banks," Scientific Journal of Financial and Commercial Studies and Research, vol. 2, no. 2, pp. 997–1044, 2021.
3. J. Slaymi, Boushi, and Youssef, "Digital Transformation Between Necessity and Risks," 2019.
4. M. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 7th ed. New York, NY, USA: Pearson Education, 2016, p. 275.
5. S. K. Thompson, Sampling, 3rd ed. Hoboken, NJ, USA: Wiley, 2012, pp. 59–60.
6. J. F. Hair Jr., W. C. Black, B. J. Babin, and R. E. Anderson, Multivariate Data Analysis A Global Perspective. London, UK: Pearson, 2010.
7. S. Berghaus, The Fuzzy Front End of Digital Transformation Activities and Approaches for Initiating Organizational Change Strategies. St. Gallen: University of St. Gallen, 2018.
8. C. Ebert and C. H. C. Duarte, "Digital Transformation," IEEE Software, vol. 35, no. 4, pp. 16–21, Jul. 2018.
9. N. G. A. Al-Anzi, "Arabic Language Teachers Attitudes Towards Using Modern Technologies in Teaching Arabic at the Primary Level in Arar City," Journal of Faculty of Education Assiut, vol. 37, no. 11, pp. 221–247, 2021.
10. E. Magerakis and A. Habib, "Business Strategy and Environmental Inefficiency," Journal of Cleaner Production, vol. 302, p. 127014, 2021.
11. M. H. Al-Fatlawi, M. F. Al-Dulaimi, and S. A. Hussein, "Total Quality Management Practices and Their Role in Sustainable Organizational Performance," Journal of Islamic University College, vol. 1, no. 63, pp. 215–254, 2021.

Vol. 21 No. 2 (2026): May
DOI: 10.21070/ijler.v21i2.1547

12. K. M. A. Al-Masri, "The Degree of Strategic Planning Practice by Secondary School Accountants in the Gaza Governorates," Ph.D. dissertation, Islamic University of Gaza, Palestine, 2011.
13. J. Hunt and M. Fitzgerald, "The Relationship Between Emotional Intelligence and Transformational Leadership An Investigation and Review," American International Journal of Social Science, vol. 2, no. 8, pp. 30–38, 2013.
14. B. M. Bass, "Transformational Leadership Looking at Other Possible Antecedents and Consequences," Journal of Management Inquiry, vol. 4, no. 3, pp. 293–297, 1995.
15. H. Al-Sharif, "Risks of Electronic Accounting Information Systems," Master's thesis, Islamic University, Gaza, Palestine, 2006.
16. M. H. Salem, "The Role of Accounting Measurement for Total Quality in Enhancing Financial Reports," Ph.D. dissertation, Sudan University of Science and Technology, Sudan, 2007.
17. S. R. Robinson and L. Volonino, Principles and Practices of Information Security. Upper Saddle River, NJ, USA: Pearson, 2004.
18. A. Khalil, "The Influential Role of Information Security Governance in Reducing Risks of Electronic Accounting Information Systems," Iraq, 2013.
19. I. Abu Shaiba, "Electronic Accounting Information Systems and Their Role in Internal Auditing," Scientific Journal, Misrata University, Libya, 2018.
20. F. Al-Ubaidi, "Risks of Using Computerized Accounting Information Systems and Their Role in the Auditing Process in Jordan," Master's thesis, Middle East University, Jordan, 2012.
21. N. Qwaider, "Internal Control Systems and Their Role in Information Security," Journal of Tripoli University, vol. 2, no. 20, 2018.

ISSN 2598-9928 (online), https://ijler.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo