E-ISSN: 2997-934X

American Journal of Business Practice
https://semantjournals.org/index.php/AJBP

| Research Article

Check for updates

The Extent to Which Accounting Disclosure is Affected by the Digital Transformation of Iraqi Banks in Light of Cybersecurity Risks and Challenges

Lecture. Anfal Saber Sharif, Lecture. Bilal Muhammad Daoud,
Asst. Prof. Dr. Samir Taha Yassin
Northern Technical University, Administrative Technical College

Abstract: The current research aims to study the extent to which accounting disclosure is affected by the digital transformation of a sample of Iraqi banks in light of cybersecurity risks and challenges. The research adopted the questionnaire as a tool for collecting data and it was distributed to a random sample that included (38) accountants. The research adopted a set of hypotheses, namely (the existence of an impact of digital transformation on accounting disclosure in the banks studied, In addition to revealing the correlation between accounting disclosure and the ability of Iraqi commercial banks to confront cybersecurity threats, the research reached a number of conclusions, the most prominent of which is (that accounting disclosure in light of the digital transformation process in commercial banks poses a major challenge due to the backward local environment in this field), It came out with several recommendations, the most prominent of which is (benefiting from the experiences of leading banks in the field of employing and managing new digital technology in a way that improves the performance of banks to carry out their work appropriately).

Key words: accounting disclosure, digital transformation, cybersecurity.

This is an open-access article under the CC-BY 4.0 license

Introduction

In the business environment, cyber risks are described as operational disruptions that lead to the loss of data or information, or the loss of privacy or integrity. Cyber risks are also described as interruptions that have a detrimental impact on business operations and an organization's IT infrastructure. Given that the majority of today's corporate transactions occur over the internet, wireless communications, and cloud computing, accounting data requires cyber protection, and financial accounting information requires comprehensive and stringent security measures.

The banking sector is one of the most important sectors in the Iraqi economy, not only for its crucial role in regulating and financing projects and various types of credit for investment projects and others, which represents the direction of economic activity in Iraq. In the event of a digital transformation, this sector will face significant challenges, some of which fall under the category of strategic change in banking operations, and others that focus on the safety, security, and disclosure of digital transactions.

Here, banks must provide a robust and flexible technological infrastructure that ensures the provision of secure, high-quality, and efficient services. Banks will be in a position that does not allow them to make rapid changes to their IT infrastructure or the structure above it. Banks' decision to add more digital solutions at all operational levels will have a significant impact on their financial stability, while not all banks are in a position to make rapid changes to their IT infrastructure or the structure above it.

On the other hand, the issue of disclosure, integrity, and security of digital information occupies a significant space in the digital transformation process of banks. Cyber attacks pose a threat to systems connected to the global network, especially in the banking sector. Then there is the issue of disclosing cybersecurity procedures and whether there are standards that determine what can be disclosed and the appropriateness of the information that can be made available to others. Reports issued in this regard indicate that the opportunities created by information and communications technologies represent a special challenge for banking institutions, as they continue to innovate in finding and providing new ways to reach customers. At the same time, these institutions are exposed to new risks, as the malicious use of information and communications technology can lead to the disruption of financial services essential to national and international financial systems, undermine security and trust, and jeopardize financial stability.

The first topic

First: The research problem

Digital banking transformation is not just a process of changing the way services are conducted. There are risks inherent in this approach, including cybersecurity challenges and the need to disclose the risks of its procedures. The research problem revolves around the impact of digital transformation in the Iraqi commercial banking sector on accounting disclosure, the challenges and difficulties represented by cybersecurity risks, and the procedures that accompany the transformation process. Therefore, the problem can be formulated as follows:

What are the implications and challenges of digital transformation for accounting disclosure of cybersecurity risks and the determinants of its measurement in Iraqi commercial banks?

Second: Study hypotheses

First hypothesis: There is a statistically significant impact of digital transformation on accounting disclosure in the banks studied.

The second hypothesis: There is a statistically significant correlation between accounting disclosure and the ability of Iraqi commercial banks to confront cybersecurity threats.

Third: The importance of research

The importance of the research stems from the fact that digital transformation in the banking sector has become an urgent necessity in light of the global shift from traditional services to providing digital services characterized by speed and efficiency. This transformation faces obstacles and challenges, the most important of which is accounting disclosure in a digital environment that is completely different from the traditional environment. The banking services provided to customers have changed. Accounting disclosure here must be different from accounting disclosure in the context of traditional work. Rather, it must disclose financial and

quantitative content about everything related to disclosure in light of cybersecurity challenges. Thus, the research constitutes a new starting point for disclosure and the expansion of its scope in light of cybersecurity risks and the determinants of its measurement.

Fourth: Research objectives

The research aims to review the theoretical research on the importance of digital banking transformation, reach conclusions on the impact of accounting disclosure on the risks involved in cybersecurity, define the concept of cybersecurity, and the role of banks in disclosing related procedures through accounting, regulatory, and management reports, in the absence of standards that determine the quality and quantity of such disclosure contained in these reports.

Fifth: Previous studies

1- Study (2017Ali et al.) "The effects of cyber threats on customer's behavior in e-Banking services) This study aims to critically analyze and discuss the effects of cyber threats when dealing with online banking services. The most important findings are that there is a need to increase customer awareness about the cyber crimes available when dealing with online banking services and sensitive financial data.

2- Study (2019).Framework for Minimizing Cyber Security Issues in the Banking Sector of Nepal (Maharjan & Chatterjee) The study aimed to analyze the cyber security issues related to the banking sector in Nepal and propose a new framework to mitigate the cyber threat.

3- study (Kitsios et al. (2021) titled "Digital Transformation and Strategy in the Banking Sector: Evaluating the Acceptance Rate of E-Services" aimed to examine the acceptability of digital transformation among banking sector employees in Greece. One of the most prominent findings is that cyber risks represent a major challenge that must be taken into consideration by employees and executives and may affect their willingness to use digital technologies. The study found that employees ignore the negative consequences of cyber attacks.

4- A study (Bress and Jabr, 2020) on digital transformation technology and its impact on improving the strategic performance of banks. The study aimed to study the impact of digital transformation technology on improving the strategic performance of banks. The most important results were that new digital technology led to increased expansion of banking markets by changing the business model that enables banks to expand their reach to customers. One of the most important recommendations was the need to benefit from the experiences of international banks in this field.

5- A study by Al-Sayed (2021) entitled "The Economics of Cybersecurity in the Banking Sector" aimed to highlight the challenges facing society in achieving cybersecurity. One of the most important results is that the continuous development of cyber risks motivates banks to conduct continuous and intensive research to take preventive measures against these risks.

6- A study by Al-Zubaidi and Al-Tamimi (2022) entitled "Iraq and Cybersecurity: Opportunities and Challenges" aimed to identify the role of cybersecurity in managing the security system files in Iraq and to provide possible solutions to enhance the concept of cybersecurity and deepen the scientific concept in the security, political, military and economic fields. The most prominent results are that information technology is at the forefront of the first and necessary demands for building secure countries in a region that has always lacked security and safety.

What distinguishes the current study from previous studies is that it relied on three variables and linked them to each other. These variables had a strong correlation in terms of influence. There is an influence between digital transformation and accounting disclosure, in addition to the relationship between accounting disclosure and cybersecurity risks.

The second topic

Conceptual Framework for Digital Banking Transformation

Conceptual Framework for Core Banking Business Models:

Banks operate with different business models based on their risk preferences, market position and comparative advantages, and each banking business model focuses on some activities rather than others (2020:28,The banking industry has witnessed the development of various business models aimed at satisfying specific markets. However, banking business models have begun to change not only under the influence of customers but also under the influence of technological developments. Instead, they face new types of competition by creating new banking business models. Regardless of the traditional models, institutions that provide financial services using fintech developments may fall into two broad business models, such as the digital bank model or the new bank model (Temelkov, 2020:10).

1.1 Traditional banking business modelTraditional bank business model: Traditional banks are facing the necessary reform measures and perhaps the biggest challenge they have faced so far in their ability to continue competing. They now have the opportunity to transform their business model into a digital banking platform or system. This will enable them to meet the requirements of the digital age in the fastest possible way (2015:16 Dapp & Hoffmann). Technological progress may lead to the vertical and horizontal disintegration of the traditional banking business model. New developments continue towards enabling machine learning and artificial intelligence through the abundance of (non-financial) data, and the dominance of digital platforms and smartphones (2020:50 Boot et al.)

2.1 Digital Banking Business ModelDigital banking can be a valuable alternative to banks in countries with less access to banking services for low-income people, as it helps overcome underdeveloped infrastructure and travel costs (Yip & Bocken, 2018:156). Traditional banks face necessary reforms, perhaps the biggest challenge they have faced so far to remain competitive. They now have the opportunity to transform their business model into a digital banking platform or system. This will enable them to meet the demands of the digital age as quickly as possible.

(2015:16 .Dapp & Hoffmann

The importance and stages of digital transformation

Digital transformation is a phenomenon that has its importance and benefits for accounting disclosure, as (Gharbi et al.: 493, 2024) (Dawoud: 2025, 103) see that the importance of digital transformation lies in:

1. Increased efficiency: Digital transformation helps automate processes, improve operational efficiency, and reduce time and effort.
2. Improving customer experience: Digital transformation enables better, more personalized customer service, enhancing customer loyalty.
3. Innovation: Digital transformation encourages innovation through the use of new technologies such as artificial intelligence and big data.
4. Competitiveness: Helping organizations adapt to a rapidly changing market and remain competitive.
5. Improve decision making: Using data and analytics to improve the accuracy and effectiveness of management decisions.

Digitization is also known as digital transformation and is a combination of both digitization and digital innovation measures aimed at improving existing products with advanced capabilities. It synchronizes the business and IT strategy of an economic unit and integrates IT into the business

strategy.Udovita 2020:522.) In general, the stages of digital transformation include three stages in general. In 1937, the German engineer (Konrad Zuse) invented the machine (21). This machine performs mathematical operations based on binary numbers, zeros, and ones. (Zuse) This revolutionary invention became the basis for almost all computer technologies that we know and use in our daily lives. (Zuse)'s invention did not only affect the world of technology (all major digital computer systems that followed (21) were based on the principle of the binary system, but it was the origin of the formulation of the phenomenon we call digitization. These stages are:

1- Digital stage (Digitization): Its mission is to convert physical assets such as data into digital data or digital objects via a scanner, camera, or any other electronic device for the purpose of processing them by a computer (Manzuch 2017:20)

2- Digitization stage (Digitalization: J. Scott Brmnen and Daniel Kreiss define it as the way in which many areas of social life are being restructured around digital communications and media infrastructures. Brmnen & Kreiss base their definition of digitalization on social life. In other words, how people interact with it. As these interactions move away from analog technologies (postal mail and phone calls) to digital technologies (email, chat, and social media), both work and leisure become digital. (Bloomberg, 2018:3)

3- Digital transformation (Digital Transformation: Digital transformation involves communication between actors such as companies and customers across all sectors of the value chain and the application of new technologies in this way. Digital transformation requires skills that include extracting and exchanging data, as well as analyzing that data and converting it into actionable information. This information is evaluated for use in various decision-making options or activities that increase the performance and scope of the company. Digital transformation includes companies, business models, processes, relationships, products, etc. (& Schallimo 2018:11 Daniel). Digitalization, also known as digital transformation, is a combination of both digitalization and digital innovation procedures aimed at improving existing products with advanced capabilities. It synchronizes the business and IT strategy of an economic unit and integrates IT into the business strategy (2000:522 ldovita).

The main stages of digital transformation in the banking sector:

The concept of digitization in the banking sectorDigitization in the banking sector means seamless performance and a hassle-free experience for customers. Digitization offers new technology-based services to its customers such as ATMs, credit cards, real-time gross settlement, electronic fund transfer, online banking, and mobile banking. (2021:126 Siemy Bloisly)

According to banking experts, digital transformation can occur in five main stages.Galazova & Maonica)

1- Adopting digital channels ATM networks: online banking, mobile banking, chatbots. The digital transformation in businesses begins. Users who want to interact with their banks through any available channels at a convenient time are at the heart of the ecosystem.

2- The emergence of digital products, big data, contactless payments, virtual cards, artificial intelligence, and machines with the help of modern advanced software, products are being created.End to end designed to meet the financial needs of customers 24 hours a day

3- Adopting a full cycle of digital services: Banks are not only adding digital services to their traditional offerings, but are also creating new digital assets, changing business models in general, and expanding their business boundaries. The use of digital tools enables them to become global.

4- Creating digital intelligence by automatically studying the "digital mind" data across all business sectors, departments, production lines, and services on an ongoing basis, giving the organization greater insight into its capabilities.

5- 5th stage creationDigital DNA - a new coordinate system for making strategic decisions throughout the bank's lifecycle.

Advantages of digital banks

The banking sector is expected to digitize to keep up with the growing expectations of the world. The increasing use of smartphones has reduced human errors and increased convenience. Cyber threats are on the rise. Hence, banks need to be highly vigilant and prepared to deal with cyber attacks. Digitization is of vital importance for data processing, storage and transmission as it allows information of all types and in all formats to be transferred with equal efficiency.Harchekar (2018:103) The most important services provided by digital banks are investments, online trading accounts, electronic money transfer, clearing services, branch networks, mobile applications and wallets. These are some of the modern products and services that act as an engine for the growth of the banking sector. Digital banks achieve many advantages, including: (2018:487.NAVEENA) and (2018:104.Harchekar)

1- Reducing costs for banks and customers through the use of ATMs, cashless transactions, etc.

2- Digital banking management allows banks to provide more digital data, enabling them to make quick, flexible decisions using digital analytics. This, in turn, benefits both customers and banks.

3- The technology is non-discriminatory so everyone will be treated the same in banks.

4- The number of customers for banks will increase due to the increased convenience of banking for them.

5- Digitization reduces human error.

6- Improving customer experience in digital transactions

7- Reduces the need to handle large amounts of cash

8- Digital banking makes opening bank accounts easier.

9- By relying on automation, repetitive tasks will be eliminated.

10- The rural-urban gap will be eliminated.

The disadvantages of digital banks are as follows:

1- Digitization reduces employee effort and thus leads to job loss.

2- Some bank branches may cease to exist as the use of online banking services increases.

3- Banks will be more vulnerable to cyber attacks.

4- Lack of privacy, as no one can hide any amount in banks.

5- High unemployment rates

The third topic

Accounting Disclosure in the Light of Cybersecurity Risks

There are many definitions of disclosure, as defined by (2017,Kurinyepa) to disclose companies on social networking sites as it is the dissemination of information via Internet technologies and information technology that supports relationships and communication between people and thus makes information available to users and interact with it in real time. Also, disclosure on social networking sites is known as providing or publishing information that constitutes the outputs of the accounting system quickly and directly in front of all investors and stakeholders who have a relationship with companies by taking advantage of modern means in the field of information and communications technology represented by creating special accounts for them on social

networking sites that enable them to reveal and display the information they wish to publish immediately (Al-Zaghbi, 2020: 179)

Researchers consider accounting disclosure as a technique used by an organization to provide information about the company, whether financial or non-financial, historical or future, to stakeholders in a way that clarifies the nature of the company's financial position, thus helping them make decisions.

Second: The importance of disclosure:

The use of social media sites allows a company to send multiple messages over time directly to a known number of followers and this is usually achieved through

Tweet messages and include Rapid in a full news release available on the company's website (2015,Miller & Skinner), 2015. Lee et al. predict that social media is an effective channel for disclosure due to two main features: megaphone (i.e., the ability to quickly deliver the intended message to a large number of users) and sharing.

Third: Disclosure objectives:

(Abdul Halim, 2017: 448) summarized in his study the objectives of disclosure through the media:

Social communication, which is:

1- Providing information of interest to stakeholders in a more clear and effective manner than information provided through mandatory disclosure.

2- Providing important information that allows users of financial statements and reports to introduce new variables and indicators into the decision-making process.

3- Improving the level of disclosure of non-financial data and presenting it with greater transparency and accuracy for the purpose of benefiting users of financial reports.

4- Reducing the information gap between financial report preparers and users of all orientations and interests.

5- Improving the organization's image and conveying positive values in its performance to stakeholders, in what is known as impression management.

Accounting Disclosure in the Light of Cybersecurity Risks

Companies and global markets have turned to using the Internet and websites to publish their financial reports and provide financial information to stakeholders, as it provides many advantages such as high speed in delivering information, ease of access to it and low cost of obtaining it, which is called online financial reports (IFR) or cyber disclosure (2019:17 .Syaeid) Companies have an incentive to manage cybersecurity disclosure strategically in the same way they do with other voluntary disclosures such as those involving business risks, some financial information, and environmental and social performance as regulatory forces push companies to disclose more cybersecurity information and to do so in a timely manner.

On the other hand, disclosing cybersecurity information may help hackers successfully attack the company, weakening the incentive to disclose. Similarly, (&D'Arcy 2022:780 Basoglu) Risk disclosure is a critical aspect of risk governance. There are concerns about the quality and adequacy of risk disclosures as executives may have incentives to underestimate exposure to cyber risks and overestimate defenses against them. Disclosing negative information about cybersecurity may increase the cost of capital and expose confidential information to both competitors and attackers. On the other hand, insufficient disclosure may leave the company vulnerable to litigation and reputational loss (McGrath et al. 2022:8).

Disclose bad news in a timely manner can protect companies from the risk of litigation (2020:18).Ashraf) Here, companies must disclose the nature of the attack, its occurrence, its cost, and its consequences. In addition to disclosing the costs of actual attacks, companies must also disclose the costs of potential attacks, which may be difficult to estimate. Cybersecurity has also become largely a matter of accounting and management review. It is subject to cost-benefit analysis, internal control evaluation, and disclosure policy considerations. According to (Gordon and Lob, 2006), cybersecurity objectives can be divided into three main categories: (Haapamäki, & Sihvonen. 2019: 809

- ✓ Cybersecurity protects the confidentiality of private information.
- ✓ Ensures that authorized users can access information in a timely manner.
- ✓ Cybersecurity protects the accuracy, timeliness, and validity of information.

The concept of cyber security: The term cyber security appeared several years after the emergence of the computer, specifically in 1972, as it was just an idea that continued until the end of the seventies of the twentieth century, and with the emergence of the first anti-virus application and its path tracking by researcher Bob Thomas, he called it (Creeper). This program was able to move across the network (Al-Khaled, 2024: 165). A number of research papers dealt with it, such as:Johan van Niekerk and Rossou von Solms (2013) defined the term cybersecurity as the protection of users and their assets from online threats. Nowadays, the concept of cybersecurity has become much more than just insecurity, becoming a real problem that requires attention and appropriate measures to ensure the safety of internet users. Cybersecurity goes beyond technical issues and has become the cause of many social problems. It can be said that cybersecurity expresses all the procedures and resources used to ensure the safety of cyberspace and cyberspace-connected systems from illegal incidents that are considered a violation of the law (Al Shamsi, 2019:9). (Abdul Aziz, 2024:203) defined cybersecurity as: the practice of protecting networks, devices, programs, and data from electronic attacks and preventing unauthorized access to sensitive data. A 2016 survey revealed that the cost of cybercrime to the global economy was approximately $450 billion. Denial-of-service attacks, infrastructure damage, and other data protection issues are a major component of highly sophisticated cyberattacks. Nearly 70% of capital market and banking executives consider cybersecurity a threat to their development. Financial institutions with legacy systems are more vulnerable to cyberattacks than others, and the cost of these attacks is lower.

Researchers knowCybersecurity is defined as: (protecting the information system from unauthorized access and modification of information, whether stored, processed, or transmitted, and protection against service interruption for users, and procedures for detecting, documenting, and responding to risks)

The effects of these attacks are also particularly significant for organizations that rely on electronic systems due to their intangible activities, which rely heavily on technology. This is due to the following reasons:

Digital Banking Infrastructure: Banks that use digital banking services are arguably classified as "innovative" and their costs are lower compared to other banks in the same sector. Therefore, the importance of the electronic infrastructure used by banks lies in the low cost of each transaction, along with the advanced infrastructure of payment and settlement systems, trading platforms, central securities depositories, and central counterparties. However, the level of customer education, including the functionality of the bank's website, is a key factor contributing to the success of online banking services (2019:19).Suleymanov et al.) Developing the electronic banking infrastructure in the right way increases responsibility and maximizes participation. The trade in banking resources will lead to economic and social well-being in society. On the other hand, the production cycle, through the allocation of banking resources to various sectors and the

infrastructure of society such as industry, agriculture, trade, health, education, entrepreneurship, etc., will lead to a reduction in unemployment, the absorption of labor, and an increase in per capita income. As a result, it will be accompanied by an improvement in the quality of life and social health of society and a reduction in poverty, which are considered indicators of economic and social development. (Mohammadi 2020: 94)

Potential challenges and threats in the digital banking sector:

1- Identity Theft: Identity theft in online banking involves the seizure of an individual's personal information to commit fraud for financial gain. It results in significant financial losses for both victims and banks.

2- phishingPhishing is one of the most common methods by which identity theft occurs in online banking. It uses fake email addresses and fake websites to trick unsuspecting customers into revealing personal information such as user IDs, passwords, credit card numbers, PIN codes, addresses, bank account numbers, etc. 2020:20 Sah

3- phishingVishing: Occurs when an attacker contacts a victim and uses social engineering to trick the victim into revealing some confidential information.

4- Cloned voice banking systemsCloned voice-banking systems: This occurs when various phishing attacks clone voice-banking systems to appear like official ones. Fake emails are used to entice customers to call a number purporting to be their bank (Abu & Matalqa, 2015:181).

5- Malware (malicious code)Malicious Malware: Malicious code (or malware) is defined as software that fulfills the attacker's intent to intentionally cause harm. Viruses can be used to damage computers and connected networks, steal information, create botnets, deliver advertisements, and steal money (Moser et al., 2009:1).

6- Hacking or hacking:(Hacking: Cracking is breaking into another party's computer devices and networks for profit, deleting data or program files, hacking into a web server, and vandalizing web pages. Hacking into computer systems to cause harm (Pathak. 2016:48)

7- Online Banking Fraud AutomationAutomating Online Banking Fraud: Cybercriminals and computer fraudsters have now taken a step forward by relying on automated transfer systems (ATSs). A new type of automated online banking fraud has begun, which is used in conjunction with variants of the Spy Eye and Zeus malware as part of a Web Inject file, a text file containing a lot of JavaScript and HTML code (Ali et al., 2017:73).

8- Security vulnerabilities:Zero Day Attack is a vulnerability exploited by Internet users and is one of the effective tools used by attackers now, because the data of a Zero Day Attack is not available until after the attack is discovered (Adil et al. 2020:3). In general, a Zero Day Attack is defined as a situation in which an attacker exploits a vulnerability that is not noticed by the administrator or developer and is considered within the context of phishing. The direct way to address this problem is to implement a mechanism that mitigates this vulnerability (Haruta 2019:2463). The Hue Signature automatic update system based on visual similarity for detecting Zero Day Attack concludes.

9- Data breach: A data breach results in the intentional or unintentional loss of secure or personal information. Data breaches can include any type of data: financial information, individual identity information, including hard drive or database information that may be stored unencrypted (2015:5).Alliance) while (Rosati 2019:2.et al) defined a data breach as an incident involving unauthorized access to sensitive, protected or confidential data resulting in a breach or potential compromise of the confidentiality, integrity or availability of the information asset as the unauthorized acquisition

10- social engineering attacksSocial engineering attacks: These are among the most dangerous threats currently facing cybersecurity. They can be detected but not stopped. Social engineers exploit victims to obtain sensitive information, which can be used for specific purposes or sold on the black market. (Luo et al., 2011:1-2). Cybersecurity has also become largely a matter of management accounting and auditing, subject to cost-benefit analysis, internal control evaluation, and disclosure policy considerations. According to Gordon and Loeb (2006), cybersecurity objectives can be divided into three main categories: Sihvonen, 2019:809, Haapamaki &)

- ✓ Cybersecurity protects the confidentiality of private information.
- ✓ Ensures that authorized users can access information in a timely manner.
- ✓ Cybersecurity protects the accuracy, reliability, and authenticity of information.

Therefore, researchers in the context of cybersecurity risk disclosure argue that if a company faces high risks and fails to inform and alert investors about these risks in advance, and these risks develop into actual cyber risks, the company may be subject to legal accountability. This motivates managers to disclose cybersecurity risks if they are aware of the likelihood of these risks being high and their repercussions being significant. However, on the other hand, managers who perceive the likelihood of a future cybersecurity event to be low and the impact of such an event to be small will be less likely to disclose cybersecurity risks. Managers are unwilling to pay to disclose negative information when the risk of lawsuits and reputational damage is low.

Section Two - The Practical Aspect

First: Variable description accounting disclosure At the level of the banks studied and diagnosed

The table data was sorted (1) There is a general agreement among the respondents regarding: variable accounting disclosure The agreement rate reached (92.62) And in the middle of my account (4.35) and standard deviation (0.81) and response rate (87.04) and coefficient of variation (18.73), knowing that. This is variable Covered a set of sub-paragraphs of (x1) to (x5) and the greatest contribution was made by paragraph (x2), which emphasized that(accounting disclosure improves The image of the institution in front of its beneficiaries), and this was with a general agreement rate of (97.3),via presentation the information that It interests stakeholders more clearly and effectively than the information provided.via Mandatory disclosure Which contributes to Improving the organization's image and exporting positive values in its performance to stakeholders Arriving at what It's called impression management.

Table (1) Description of the accounting disclosure variable

Response measurement														
Response rate %	Coefficient of variation %	Standard deviation	Arithmetic mean	No I strongly agree		No I agree		Neutral		I agree		I strongly agree		Questions	
				%	T	%	T	%	T	%	T	%	T		
83.60	19.86	0.83	4.18	2.6	1	2.6	1	2.6	1	57.9	12	34.2	13	X1	accounting disclosure
91.60	12.01	0.55	4.58	0	0	0	0	2.6	1	36.8	14	60.5	23	X2	
87.40	13.73	0.60	4.37	0	0	0	0	5.3	2	42.1	16	52.6	20	X3	
85.20	27.23	1.16	4.26	7.9	3	2.6	1	0	0	34.2	13	55.3	21	X4	
87.40	20.82	0.91	4.37	2.6	1	2.6	1	5.3	2	34.2	13	55.3	21	X5	
87.04	18.73	0.81	4.35	2.62		1.56		3.2		41.04		51.58		General average	
				4.18						92.62				Overall average of the dimension	

Source: From numbers Researchers in a light Program results Analysis statistician spss26

Second: Describing and diagnosing the digital transformation variable at the level of the banks surveyed.

I explained Table data(2) There is a general agreement among the respondents regarding: Digital transformation variable The agreement rate reached (92.12) with an arithmetic mean of (4.41), a standard deviation of (0.83), a response rate of (88.20), and a coefficient of variation of (18.92), noting that this variable It included A set of subparagraphs from (Y1) to (Y5) and the greatest contribution was to paragraph (Y1), which emphasized that(The organization under study uses Digital data enables them to make important decisions.), and this was with a general agreement rate of (94.7),so Digitization helps open bank accounts, as well as Reduce costs Organization-relatedand customersvia During the use of ATMs and non-cash transactions Providing the ability to deal with the customer's bank account through several banks in different locations.

Table (2) Variable description Digital transformation

Response measurement															
Response rate %	Coefficient of variation %	Standard deviation	Arithmetic mean	No I strongly agree		No I agree		Neutral		I agree		I strongly agree		Questions	
				%	T	%	T	%	T	%	T	%	T		
87.40	13.50	0.59	4.37	0	0	0	0	5.3	2	52.6	20	42.1	16	Y1	Digital transformation
92	20.87	0.96	4.6	2.6	1	5.3	2	0	0	18.4	7	73.7	28	Y2	
89	14.61	0.65	4.45	2.6	1	2.6	1	2.6	1	39.5	15	52.6	20	Y3	
87.40	23.34	1.02	4.37	5.3	2	2.6	1	0	0	34.2	13	57.9	22	Y4	
85.20	22.30	0.95	4.26	2.6	1	5.3	2	2.6	1	42.1	16	47.4	18	Y5	
88.20	18.92	0.83	4.41	2.62		3.16		2.10		37.36		54.76		General average	
				5.78						92.12				Overall average of the dimension	

Source: From numbers Researchers in a light results program Analysis statistician spss26

Third: Description and diagnosis of the cybersecurity variable at the level of the banks studied

The data in Table (3) showed that there was a general agreement among the respondents regarding the cyber security variable, as the agreement percentage reached (92.26), with an arithmetic mean of (4.44), a standard deviation of (0.78), a response rate of (88.72), and a coefficient of variation of (17.57). It is worth noting that this variable included a group of sub-paragraphs from (Z1) to (Z5), and the greatest contribution was to paragraph (Z3), which confirmed (Cybersecurity seeks to protect computers and the networks connected to them from being accessed by malicious software or hackers.), and this was with a general agreement rate of (94.8), in addition to the fact that cyber security works to protect against the seizure of personal information.coupled with disclosureAbout the risks of revealing cybersecurity information to hackers.

Table (3) Variable description Cyber security

Response measurement															
Response rate %	Coefficient of variation %	Standard deviation	Arithmetic mean	No I strongly agree		No I agree		Neutral		I agree		I strongly agree		Questions	
				%	T	%	T	%	T	%	T	%	T		
89	14.61	0.65	4.45	0	0	0	0	9.7	3	39.5	15	52.6	20	Z1	Cybersecurity
87.80	24.60	1.08	4.39	5.3	2	2.6	1	0	0	31.6	12	60.5	23	Z2	
86.80	13.36	0.58	4.34	0	0	0	0	5.3	2	55.3	21	39.5	15	Z3	
91	20.88	0.95	4.55	2.6	1	5.3	2	0	0	18.4	7	73.7	28	Z4	
89	14.38	0.64	4.45	2.6	1	5.3	2	0	0	39.5	15	52.6	20	Z5	
88.72	17.57	0.78	4.44	2.10		2.64		3		36.86		55.40		General average	
				4.74						92.26				Overall average of the dimension	

Source: From numbers Researchers in a light results program Analysis statistician spss26

Fourth: Testing the impact of digital transformation on accounting disclosure in the banks studied

Indicates The content of this relationship is to test the main research hypothesis. First that It was statedon There is a statistically significant effect for For digital transformation On aFor accounting disclosure In the banks under study,so It is clear from the table(4)Having a moral effect For variable AFor digital transformation In accounting disclosure, the significance level value was(0.000)It is less than the hypothetical moral level of the study.(0.05)And explained variable AFor digital transformation In terms of the coefficient of determination(R2)What is its percentage?(0.52%fromDifferencesCollege of Accounting Disclosure inbanks The researched, and supports his moral value(F)The calculated(67.33)It is greater than its table value.(4.35)at two degrees of freedom(1,36)and morale level((0.05and the remaining percentage of(0.48%)It is due to other variables that cannot be controlled or were not included in the research plan, and the value of the regression coefficient reached(Beta) (0.72)It is a moral value in terms of meaning.(t)The calculated(8.20)It is greater than its table value.(1.68)At a moral level((0.05, which indicates that the change in AFor digital transformation By one unit, it will change the percentage.(0.72)from Accounting disclosure in the banks studied These results indicate the acceptance of the main hypothesis .First To search for text Ton There is a statistically significant impact of digital transformation .on Accounting disclosure in the banks studied.

Table (4) Impact transformation variable Digital accounting disclosure

Trans formation Digital						independent variable
T		B	F		R^2	Analysis data / dependent variable
Scheduled	The calculated		Scheduled	The calculated		
1.68	8.20**	0.80	4.35	67.34**	0.52	الإفصاح المحاسبي

Source: Prepared by Researchers In light of the resultsprogramSPSS26 df = 1,36 n=38 **P ≤ 0.05

Fifth: Testing the nature of the correlation between variables Accounting Disclosure and the Ability of Iraqi Commercial Banks to Confront Cybersecurity Threats

This analysis aims to test the correlation between the two research variables, namely: accounting disclosure and Cybersecurity(Depending on the correlation coefficient)Person-Correlation The content of this analysis indicates the testing of the second main hypothesis, which states that there is a statistically significant correlation between...For accounting disclosure and The ability of Iraqi commercial banks to confront Cyber security threats, and by following the data of Table (5), it becomes clear that there is a statistically significant correlation between them, as indicated by the value of the correlation coefficient between them, which is (0.86) and at a significant level(0.05These results indicate the significance and strength of the correlation between the two variables, indicating the acceptance of the second main hypothesis, which confirms the ability of the variable accounting disclosure In explaining the possibility Iraqi commercial banks face cybersecurity threats And predict it.

Table (5) Results of correlation relationships between accounting disclosure and Cybersecurity

sig	accounting disclosure	Variable The approved / Variable The mediator
0.000	0.86**	Cybersecurity

Source: Prepared by researchers in light of the results of the programSPSS26 **P≤0.05 n=38

Conclusions:

1- Accounting disclosure in light of the digital transformation process in commercial banks represents a major challenge due to the lagging local environment in this area.

2- The digital transformation process in commercial banks requires serious steps to transform the process from the banks themselves as well as from the entities responsible for managing the banks.

3- The digital transformation process in commercial banks is leading to increased customer access, as banks and other financial institutions leverage digital technology to significantly expand their reach. It also leads to reduced staffing costs due to the reliance on automation to deliver services.

4- The digital transformation process in commercial banks leads to better control over information, which leads to smarter, more timely decisions, more control over information, and less repetition of information errors.

5- Accounting disclosure in light of the digital transformation process in commercial banks represents a major challenge due to the lagging local environment in this area.

6- The most important results of the current study are that it directly addresses the impact of the digital transformation of commercial banks on accounting disclosure in light of cybersecurity risks and the implications of this impact. Previous studies did not address the relationship between accounting disclosure and the risks resulting from cybersecurity risks.

Recommendations:

1- Government institutions, including the Ministry of Higher Education, should reinforce the steps taken by government agencies in the field of cybersecurity in general.

2- The economic unit must work to follow a balanced policy as a balance in cyber disclosure. Through this policy, it must determine the degree of disclosure or the areas of disclosure.

3- Faculties of management and economics, particularly the accounting and banking finance departments, should add cybersecurity courses to their curricula and encourage scientific research in this field.

4- Cooperation between regional and international banks in the field of digital transformation and cybersecurity to implement the transformation process.

5- We must benefit from the experiences of leading banks in the field of employing and managing new digital technology in a way that improves the performance of banks to carry out their work appropriately.

Retraces:

1. Al-Zaghbi, Abdullah Muhammad Irqibat, Anwar (2020), The impact of disclosure on social networking sites “Facebook” on the trading volume of public shareholding companies listed on the Amman Stock Exchange, Arab Journal of Management, Arab Administrative Development Organization, Volume 40, Issue 4, pp. 177-190

2. Ismail, Essam Abdel Moneim Ahmed, and Al-Deeb, Mohamed Mahmoud Ibrahim, (2017), Evaluating the impact of applying the unified electronic system for accounting disclosure in the Egyptian stock market on the investment decision: an applied study. The Egyptian Journal of Business Studies, Vol. 41, No. 3, p. 604.

3. Al-Zubaidi, Zuhair Khadir Abbas, Al-Tamimi Dhafar Abdul Matar. (2022). Iraq and Cybersecurity.. Opportunities and Challenges. Wasit Journal for Humanities, Volume 18, Issue 51.

4. Al-Shamali, Hussein Ali Qasim (2017) Information Security and Confidentiality and Its Impact on Banking Performance: An Applied Study on Banks Operating in Jordan, Al-Quds Open University Journal of Administrative and Economic Research and Studies, Volume 2, Issue 7.
5. Press, Ahmed Kazem, Jabr, and Rawd Qasim (2020) Digital transformation technology and its impact on improving the strategic performance of the bank (research) Analytical viewpoints of a sample of managers working in the private commercial banking sector in Karbala, Iraqi Journal of Administrative Sciences, Volume 16, Issue 65
6. Ali, Shurooq Abdul, Khadir Ardan Hatem (2020) "Digital transformation of banking operations as a tool for developing the strategic financial performance of the Bank of Baghdad as a model", Journal of Administration and Economics, Issue 126
7. Abdel Aziz, Magda Abdel Majeed, 2024, Integration between Cloud Computing and Cloud Accounting to Ensure Cybersecurity of Financial Data: A Theoretical Study, Northern Technical University Journal for Administrative and Human Sciences, Special Issue
8. Al-Khaled, 2024, Assessing Cybersecurity Awareness: A Survey Study in the College of Administration and Economics, University of Mosul, Northern Technical University Journal for Administrative and Human Sciences, Volume 4, Issue 4
9. Gharbi, Mohammed Hussein, Danouk, Ahmed Abdullah, Zainal, Wissam Sami Jabbar, 2024, Digital transformation and its impact on green human resource management practices: A survey study of the opinions of a sample of employees at the Northern Technical University: Al-Hawija Technical College, Northern Technical University Journal for Administrative and Human Sciences, Special Issue.
10. Dawood, Razzaq Hussein Abdul, 2025, Digital leadership and its relationship to digital transformation in Iraq, Baghdad Municipality as a model, Journal of Leadership Thought for Research and Studies, Issue 1
11. Carletti, E., Claessens, S., Fatás, A., & Vives, X. (2020). Barcelona Report 2-The Bank Business Model in the Post-Covid-19 World. Center for Economic Policy Research.
12. Temelkov, Z. (2020). Differences between traditional bank model and fintech based digital bank and neobank models. SocioBrains, International scientific reference online journal with impact factor, (74), 8-15.
13. Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2015). Fintech reloaded – Traditional banks as digital ecosystems. Publication of the German original, 261-274.
14. Boot, A. W., Hoffmann, P., Laeven, L., & Ratnovski, L. (2020). Financial intermediation and technology: What's old, what's new?.
15. Yip, A. W., & Bocken, N. M. (2018). Sustainable business model archetypes for the banking industry. Journal of cleaner production, 174, 150-169.
16. Udovita, PVMVD (2020). Conceptual review on dimensions of digital transformation in modern era. International Journal of Scientific and Research Publications, 10(2), 520529.
17. Bloomberg, J. (2018). Digitization, digitalization, and digital transformation: confuse them at your peril. Forbes. Retrieved on August 28, 2019.
18. Schallmo, A., & Daniel, R. (2018). Digital Transformation Now! Guiding the Successful Digitalization of Your Business Model. Springer Science+ Business Media, LLC.
19. Harchekar, J. S. (2018). Digitalization in banking sector. (IJTSRD).ISSN.2456-6470

20. Syaeid, T. A. (2019). The Effect of the Reliability of Accounting Information Systems on Electronic Disclosures on the Stock Prices: Applied Study on Industrial Companies Listed on Amman Stock Exchange. International Journal of Economics and Finance, 11(8), 1-14.)
21. D'Arcy, J., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. Journal of the Association for Information Systems, 23(3), 779-805.
22. McGrath, V., Sheedy, E., & Yu, F. (2022). Governance of cyber security.
23. Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. Int. J.Inf. Technol. Lang. Stud, 3(2), 8-29.
24. Mohammadi Raisi, M. Z., Fathi, S., & Karimian, H. (2020). The Developments of the Electronic Banking (E-banking) Industry, A Step towards Achieving Sustainable Development. IAU International Journal of Social Sciences, 10(4), 85-95
25. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity accounting research. Managerial Auditing Journal, 34(7), 808-834.