International Journal of Studies in Business Management, Economics and Strategies
Volume 3, Issue 8, August - 2024
ISSN (E): 2949-883X
Scholarsdigest.org

AUDITING CYBER SECURITY RISKS AND ITS IMPACT ON AUDITING PROCEDURES IN IRAQI BANKS (BAGHDAD NATIONAL BANK AS A MODEL)

Mushtaq Ali Dhiab Hussein
Asst. Prof. Dr. Ali Muhammad Thajil Al-Mamouri
University of Baghdad - Higher Institute for Accounting and Financial Studies
mym15101977@gmail.com
mushtaq.ali1101a@pgiafs.uobaghdad.edu.iq

Abstract
Iraqi banks have a technical development in providing banking services and the purpose is to link cyber security risks and audit procedures to the tasks and responsibilities of the auditor and to identify the most important threats and address them The most important conclusions reached are that there is a relationship between cyber security risks and the professional responsibility of the auditor, the most important of which is that most financial and banking entities have not identified or disclosed cyber security risks and the absence of a binding law or legal framework, which affects the audit procedures and the opinion of the auditor. This affects the professional responsibility of the auditor, as well as the failure to disclose these risks, which exposes them to threats. These risks and procedures in cyber security were not addressed in corporate laws, and the most important recommendations were to amend the laws or issue a law or framework obligating financial entities and banks to identify cyber security risks, as well as the auditor's audit program for the purpose of identifying cyber threats and risks and the most important measures taken by governance and in terms of keeping pace with the technical cyber development in order for the procedures to be at the level of the role that creates an environment of trust between him and the users of the reports and obligating the auditor through laws or instructions to exercise the necessary professional care to identify these risks as they are important risks for all Companies and proposed a cyber-security risk audit program according to the Iraqi environment .

Keywords: cyber security. Auditing procedures.

Introduction

Iraq is one of the targeted countries that are exposed to cyber-attacks, as well as financial inclusion in banks, digital transformation and automation in all state institutions and the private sector. This is a reason for developing and implementing a robust cyber security plan backed by laws and instructions that are legislated to support the implementation and application of cyber protection. From here, interest began to search and investigate the existence of... A program or framework to identify cyber security risks and the measures taken by Iraq according to the international classification for the purpose of benefiting and

updating information for all internal and external auditors regarding audit procedures and the role of the external auditor in enhancing audit procedures in Iraqi banks to ensure the integrity of data and protect it from cyber-attacks. They must also remain prepared. To update their methods and use technology to confront advanced cyber threats. Our study consists of four sections, where the first section will be the research methodology, the second will be the theoretical framework for cyber security risks and audit procedures, the third will be the practical section in the Bank of Baghdad, and finally the fourth section will be conclusions and recommendations for the purpose of identifying the most important cyber risks and their reflection on auditing procedures in Iraqi banks. .

The methodology of Research

Research problem: Research problem

The problem of research is the increase in cyber threats facing banks, such as hacks, electronic threats, and data theft, whose work has been transformed from traditional to electronic, and these risks affect audit procedures.

Research importance:

The importance of research shows the importance of information technology and identifying cyber risks and its role in advancing business resources, as attackers can access sensitive financial information such as customer information and credit card information, and this can lead to violating customers' privacy and stealing their identities and bank accounts. Financial card data can also be used to commit fraud or unauthorized purchases, and in turn, these breaches can cause significant financial losses for financial companies due to compensating those affected and repairing their compromised security systems; The reflection of these risks and previous violations may lead to a decrease in customer confidence in the bank or financial institution, causing the loss of customers and negatively affecting its reputation. To prevent this, financial companies and institutions must take strong security measures to protect their financial data, and prepare audit procedures that are proportionate to the extent of cyber risks .

Research Objectives: Research Objectives

1. Understanding the impact of cyber on audit operations: by studying how cyber security risks affect audit operations and the ability to detect possible imbalances and manipulations in accounts.
2. Achieving a balance between security and efficiency: Finding the ideal balance between enhancing cyber security and ensuring the efficiency of audit operations without negatively impacting audit procedures is the professional responsibility of the auditor.

Research hypothesis

The research was based on the basic hypothesis that (there is an influence relationship between cyber security risks and audit procedures.

Research method

In this research, the researcher relied on the descriptive approach in the theoretical framework to achieve the research objectives, and he also relied on the analytical approach in the practical framework and to obtain results.

Research Population and Sample

Research community: Baghdad National Bank was selected

Research sample: The bank's annual reports for the period (2018 – 2023) were (5) years in order to be sufficient to achieve good results.

Means of collecting data and information: Means of collecting data and information

The theoretical aspect: We relied on local, Arab and foreign sources, including books, dissertations, theses and research published in Arab and foreign journals or available in various libraries or on the Internet.

The practical aspect: annual reports issued by the Bank of Baghdad (the bank in question) during the research period.

The statistical methods used:

The research included a set of statistical metrics used to measure cyber risks

Previous studies:

researcher , Al-Ahmadi (2023)	
Auditing the comprehensive electronic banking system to detect operational business risks	**Study title**
In light of the development taking place in the environment Banking and increasing reliance on electronic systems	**Study problem**
Comprehensive electronic system application	**For study purposes**
Increased operational risks in Iraqi banks that provide electronic services, as well as the ability of banks to develop operations Banking	**The most important conclusions**
High investment in information technology with a comprehensive system The .banker	**Study recommendations**

(Ahmed. 2023)	**researcher**
Attacks on computer networks in international humanitarian law	**Study title**
There are no provisions, texts, or legal documents that address cyber attacks and threats	**Study problem**
Legal texts for protection in cybersecurity (strategy - confidentiality - privacy (enhancement -	**For study purposes**
Lack of legal texts for protection in cybersecurity	**The most important conclusions**
Finding and organizing agreements and binding law for all countries regarding attacks and protection in the areas of cybersecurity	**Study recommendations**
(praiseworthy, 2023)	**Search name**
The impact of cyber security on organization performance	**Study title**
Iraqi organizations face a problem represented by the limited application of cybersecurity and effective use of it in their organizations	**Study problem**
What are the difficulties he faces ? Organization in the field of cybersecurity Confidentiality - Privacy – Enhancement	**For study purposes**
Identify the organizational difficulties in the field of cybersecurity	**The most important conclusions**
Conduct more research on the impact of cybersecurity on companies and organizations	**Study recommendations**

The conceptual framework of the concept of cybersecurity and its reflection on the measures taken to reduce risks.

Conceptual framework of the concept of cybersecurity/

Definition of cyber security: Cyber security:

Cybersecurity is "the protection of networks, information technology systems, and operational technology systems, and their software components, the services they provide, and the data they contain from any penetration, disruption, modification, entry, use, or illegal exploitation. The concept of cybersecurity includes information security, electronic security, and digital security." And so on" (Middleton, 2017: p 3.(

As for the American National Institute of Standards and Technology, it defined cybersecurity as: "protecting from damage and restoring computer systems, electronic communications systems, electronic communications services, wire communications, and electronic communications, including the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-violation," and defined cyberspace as " A global field within the information environment, consisting of an independent network of information systems infrastructure, including the information network, communications networks, computer systems, and embedded processors. The American National Institute of Standards and Technology defines cybersecurity as "it aims to protect computer systems from illegal access." Or tampering with information during storage, processing, or transmission, also aims to protect against disruption of service to legitimate users, and cybersecurity is concerned with the necessary means to discover, document, and repel all of these threats." "It is clear that the definition of the Communications and Information Technology Commission is more comprehensive and more accurate in scientific and practical terms than the Institute." National Standards and Technology Institute of the United States." (Morgan & Stocken 1998 (pp.365-385).

Importance of cybersecurity:

Cybersecurity protects data from attackers who seek to cause harm when stealing information, as the data may be sensitive, such as private or government information; Or industrial, having mechanisms to defend infrastructures in society is as important as protecting hospital data; and service programs that are of interest to society. At the individual level, cybersecurity protects personal data. It helps to limit identity theft and blackmail attempts, which cause harm to an individual's life. As a user of the World Wide Web or social networking sites, the person should activate the privacy option for his personal information, such as age, gender, and place of residence. It is not only about sharing information, but rather what the person allows to grant the possibility Applications to access information. An application often requests access to information before starting to use it, as it could be access to the microphone, contacts, photos, and location. Cybersecurity is the process of protecting systems, networks, and programs against digital attacks. These cyber attacks usually aim to alter, alter or destroy sensitive data; For the purpose of seizing money from users or interrupting normal business operations (Al-Sharif. Mustafa Kamel 2024: pp. 10-11)

Cybersecurity purposes

Citizens of cybersecurity purposes are all of the following: (Al-Sharif; Mustafa Kamel; 2024: p. 19)

1-Protecting personal information and data from leakage and theft. Personal data is one of the most important commodities in the digital age. If the virus is able to penetrate, they are able to gain access to sell this data.

2 -Protecting businesses by preserving and protecting the confidentiality of information and privacy for individuals and companies and protecting businesses. The most important advantage is that the best cybersecurity solutions for IT security can provide comprehensive digital protection for all types of businesses. This will allow the user to browse the network, and indicate that they are not exposed to potential threats in terms of data theft. .

Benefits of cyber security

Cyber security is crucial; Ensures that IT systems are protected from cyber threats such as fraud or spying; The benefits of cyber security can reduce these effects and reduce the damage resulting from potential damage; Its most important benefits:

1-Save data approved by institutions; Or improved companies with the right security in place globally

2 -Adding confidence to employers in organizing network security in institutions.

3 -Reducing data recovery times in the event of unauthorized access to networks or systems.

Concept of cyber threat:

Financial markets represent increasingly important and attractive targets for cybercriminals, and as governments enhance the safety of all electronic services, the spread of digital financial services by increasing connectivity between banking systems and financial markets increases the threats that cyber-attacks have on financial sectors in developing countries as well as on a global level. It is considered constructive. Strong flexibility on the information network is extremely important for market stability as well as achieving financial inclusion. Cyber-attacks can restrict financial inclusion efforts because if these attacks and hacks succeed, they may lead to failure or deter customers from new electronic financial services and products. Electronic risks are considered a form of cyber security risks. Operational loss is defined as the loss resulting from successful digital incidents from internal and external incidents or third parties, including theft, compromised information, damage to information or technology assets, internal and external fraud, and business interruption. The goal of cyber risk management is as follows: (2022: P61 Strong, Welburn)

Auditing procedures in accordance with international auditing standards:

Auditing is one of the basics that currently meets the objectives of financial organizations, as scientific recommendations in most countries of the world require that importance be given to the role played by auditing as it represents an independent evaluation approach. It contributes to supporting the effectiveness and efficiency of activities. Ensure the implementation of laws, policies, and instructions. Judgment on risk management policies, perhaps increasing attention; The focus on the effectiveness of this function is largely related to modern concepts imposed as a reality for governance and risk management. And the concepts of quality and excellence that the organization’s management seeks to achieve, as

the oversight function is an important means of achieving management objectives, especially oversight ones (Ronen Cherny 20022 6-29)

"The audit function has been adopted in the modern business environment as a major support function for both users, governance, and the external user, and through the accreditation of the external auditor to benefit from the internal auditor and see the results of the business evaluation and its effectiveness." (Al-Husseini; Al-Maamouri, 2022: p. 15.)

Oversight bodies should play an important role in distinguishing the activities of the units subject to them, as one of the roles played by these bodies is to limit fraud, fraud, and violations, detect them when they occur, and take corrective and deterrent measures against them with the required speed. (Al-Shawabkeh, Abdullah Ahmed; 2007: p. 35).

The capabilities and level of development of oversight bodies can be determined from the AFROSAI institutional standard, which can be used as an evaluation tool, identifying areas for improvement, and for the purposes of balancing reference between oversight and auditing bodies.

Concept and definition of auditing:

The word "audit" is derived from the Latin word "audit," which means "to listen," because "the accounts were recited to the auditor. The recording and auditing processes improved after the accounts were organized on the basis of the dual method that was published in the book of the Italian scientist Luca Paciolo, which appeared in the city of Venice in the fifteenth century, in the year 1494 AD." (Abdulaziz; Al-Sayyid Mustafa; 2021: p. 34(

The emergence of auditing is a result of economic development and its departure from the space of individual projects to the world of large projects. Governance's urgent need to provide an important means to help it accomplish its tasks played a major role in creating this type of audit within the units. As the size of these units grows and their degree of complexity increases, it leads to increased interest in auditing as an essential element of unit control (Bethaux, A. (2000), p. 61)

Auditing, in its simple sense, is nothing more than an act carried out by individuals to ensure the correctness of the performance of the work of other individuals. Accordingly, it must be performed in a manner that takes into account certain principles, and the audit is carried out in light of those principles. The person carrying out the audit must be other than the one who carried out the implementation, and he must be on the same page. Abundant experience of knowledge and knowledge of the nature, activity, and work and how to carry it out until a judgment is reached on the accuracy of the information and its performance, otherwise there is no need for scrutiny (Talal; Muayyad Ibrahim; 1983: p. 14.)

Auditing in light of electronic processing:

The use of automation to complete the audit work by the auditor and benefit from the capabilities of the computer in carrying out these work accurately, quickly and at a lower cost, as it enables him to use computer programs to study and verify the required data, test and audit samples, and take the necessary steps to collect evidence and help him in implementing logical and arithmetic tests, as the computer has facilitated The auditor has the process of verifying the correctness of previous procedures at a value less than the value of manual performance, and the use of automation in managing accounting information has led or contributed to achieving the following purposes: (Raymod; Shibl George, 2006: p. 27).

A - Economy: The auditor works with the computer to prove that he used the maximum possible energy to serve the unit, with the least expenses, and with the availability of information. And the required data in a timely manner, which benefits the unit.

B - Effectiveness: The auditor works to effectively perform the control tools to verify the efficiency of the control system in all activities.

T - Efficiency: The controller should verify that the computer is used to complete the most important requirements and work on what is related to the unit according to the role of relative importance.

D - Protection: The auditor must work to protect the system from all risks associated with its use, the most important of which is the loss of the system and data stored on disks or other storage devices, virus problems, theft, or intentional sabotage to which the systems may be exposed, to cover violations that may be committed by some workers within the unit. Economic.

Practical (applied) aspect

First: Analysis of the annual reports of management and the auditor (research sample)

Bank of Baghdad :

First - The date of the establishment of the bank: - It is an Iraqi private joint stock company that was established on 02/18/1992 pursuant to the founding license numbered (4512) as the first private Iraqi bank, and its main headquarters is in the city of Baghdad and its fully paid-up capital is 300 billion Iraqi dinars, which was increased by issuing Bonus shares numbering (50) billion shares pursuant to the decision of the General Assembly on 11-22-2023. The bank provides all banking and financial works related to its activity through its main center in the city of Baghdad (Karada district), and its 35 branches. It is spread within Iraq and the Lebanese Republic branch (Beirut branch), in addition to providing banking and financial services, and the bank's shares are fully listed on the Iraq Stock Exchange."

Second - The capital of the bank: - The capital of the bank was determined to be (300) billion dinars.

Third - the purposes of the bank- :

1 -Maintaining a good level of key financial ratios within the requirements of the regulatory authorities, most notably maintaining the capital adequacy ratio and legal liquidity, which are not less than the requirements of the regulatory authorities.

2 -Maintaining the bank's competitive position at the level of the Iraqi banking sector and enhancing the bank's share in liability and asset products within acceptable risks and returns.

3-Enhancing the quality of the bank's assets by reducing non-performing assets and covering them with allocations that comply with international standards, by raising the coverage ratio of non-performing assets.

4 -Enhancing and diversifying investments in low-risk assets with acceptable returns through expanding government credit through local and international bonds and treasury bonds.

5-Continuing to grow revenues and control expenses in a way that contributes to improving the bank's operational efficiency

The market and customer axis for developing the bank's developmental role in the field of financing and foreign trade services, whether for the individual sector, large companies, or the government sector, through a specialized team with high professional competence, and

the bank's obtaining an evaluation from one of the international institutions in order to support this trend.

6 -Strengthening the bank's presence through opening branches and deploying ATMs in the targeted locations.

7 -Enhancing and developing electronic and digital services for customers of the Azizi Bank, regardless of their segments, and improving the concept of self-service, and providing services easily that suit their needs and aspirations at different times by developing the services provided through the bank's application on mobile phones.

8-Continuing to develop operations by working on the bank's business centers and transforming the branches into points of sale for optimum customer service.

9-Implementing a group of technical projects to help develop services and speed up their offering by relying on modern technologies.

10-Continuing to empower and develop the work team and improve the performance of human resources by enhancing the learning and development process through specialized training and enhancing administrative competencies in line with the bank's strategic directions.

Fourth - Activities and tasks carried out by the bank: - The Company practices the following activities: Activities the determinants of economic activity are still incompletely defined globally and locally, and the consequences of this at the level of business sectors. And the state of uncertainty is high, but during the year 2023, the Bank of Baghdad continued to strengthen its position and position as a leading bank in the Iraqi banking sector within the abnormal circumstances, as it worked to create opportunities from these challenges and circumstances and transform danger into possibilities and setbacks into strength. At the level of the financial framework, it was seized. Opportunity and expansion in the field of investments, as the bank in 2023 invested in Iraqi construction bonds and obtained them with an excellent return, in addition to working to reduce risky assets through collection with credit portfolios and other assets, as well as investing in treasury transfers with a maturity of one year, months and one year, and on the other hand The bank's latest work is to enhance the quality of its assets by increasing the provisions for expected credit losses for its financial assets through the continued application of the IFRS 9 standard. As for its services to customers, the Bank of Baghdad has taken on its responsibility to manage its business with all efficiency and ability and has adopted a precautionary business strategy that ensures the sustainability of the business. It maintains sustainable growth and stability with the highest standards of risk management during the crisis period, as it carried out all its banking operations in all its branches in a way that serves customers. This was accompanied by the bank's continued approach to continuous development and modernization to support its path of success and excellence, as the bank continued to create new services and products and develop existing ones in its effort towards Further improving customer experience and emulating their aspirations and ambitions through adopting and implementing projects and work programs aimed at simplifying its procedures and developing the flow of operations. The bank was also keen to keep pace with the latest technological developments in electronic applications and alternative channels for digital transformation by enhancing its electronic services and electronic distribution channels. Expanding the spread of automated teller

machines at the level of all governorates in order to achieve operational efficiency. The bank will also work to continue focusing on managing the sources and uses of its funds with the required efficiency with the aim of maximizing the profit margin and maintaining cash liquidity with continuous continuity. The vision of the Bank of Baghdad during the year 2023 aimed to work on implementing Part of its plan, according to its main axes, which focuses on developing the bank's operations and technology axis, in addition to structuring and developing individual and corporate services through the implementation of a number of projects aimed at raising the level of the bank's services and keeping pace with developments in the banking industry. This vision has resulted in achieving a group of Achievements through the implementation of a group of projects that had the impact of creating a qualitative shift in the services provided; and the development of risk management programs through the addition of the operational risk management program (Nucleusl), and on the customer side; The market has been redeployed to some branches within the Republic of Iraq, in addition to the re-evaluation of the bank with major international companies (CI), the results of which are expected to be completed before the end of the first half of the year 2023, and the start of the COBIT information governance project.

The questions were adopted within six axes mentioned in (2) below, as they will be matched with management reports and external auditor reports for the purpose of identifying the extent of the research sample's commitment to statistical systems to identify the most important results, recommendations and axes as follows:

Through these inquiries, they were matched in the management reports and the auditor's reports and are attached in the tables below. Table No. (7) Below represents the banks and years investigated, as follows:

Table No. (1)

Statistical code	Applied research themes	Statistical symbol	The bank
M1	The first focus of the study	Bank of Baghdad B	
M2	second focus of the study		
M3	The third focus of the study		
M4	The fourth focus of the study		
M5	The fifth focus of the study		
M6	Sixth focus of the study		

Bank of BaghdadB Table No. (2)

2023	2022	2021	2020	2019	2018	The first axis The role of governance in managing cybersecurity risks
1	1	1	1	1	1	1. The bank Owns that He should Cyber Security Risks To manage system .
1	1	1	1	1	1	2. The bank Owns that He should To reveal Integrated electronic system . Its occurrence before Electronic Attacks

1	1	1	1	1	1	3. The bank Owns that He should Risks To analyze electronic system . Cyber Security
3	3	3	3	3	3	the total
1	1	1	1	1	1	Rate
						The second axis (adherence to the strategy and compliance with Sirani's confidential security standards and (procedures
1	1	1	1	1	1	1. legislation Availability bezel And how much Cyber Security regulates . With it The bank commitment
0	0	0	0	0	0	2. or strategy Availability bezel Security To manage local framework of commitment and the extent Cyber . With it The bank
0	0	0	0	0	0	3. Local Standards presence bezel And how Cyber Security To manage With it The bank commitment much
1	1	1	1	1	1	4. For The bank compliance bezel To manage International standards Cyber Security
1	1	1	1	1	1	5. The bank commitment bezel) Cyber Security With elements , Information availability , confidentiality .(integrity
3	3	3	3	3	3	the total
0.6	0.6	0.6	0.6	0.6	0.6	Rate
						Structure saving) Third Axis And qualification Infrastructure and informatics Humanity Capabilities (cyber For security
1	1	1	1	1	1	1. structure Availability bezel Risks To manage Integrated Substratum Cyber Security
1	1	1	1	1	1	2. mankind Cadres presence period Risks To manage And efficient Eligible . Cyber Security
1	1	1	1	1	1	3. And Integration presence bezel For complete My information absorb before from Cyber Security system . Attic staff Individuals
3	3	3	3	3	3	the total
1	1	1	1	1	1	Rate
						Fourth Axis (Achieving banking competitive advantage in light of (cybersecurity
1	1	1	1	1	1	1. The bank in trust presence bezel His after His clients before from To Integrated system commitment . Cyber Security Risks manage
1	1	1	1	1	1	2. High responsible presence bezel after The bank Origins on The diaper in To Integrated system His commitment . Cyber Security Risks manage
1	1	1	1	1	1	3. For satisfaction presence bezel after The bank Services on customers

						To Integrated system His commitment . Cyber Security Risks manage
0	0	0	0	0	0	4. substitute system presence bezel condition in Cyber Risks To manage Guaranteed present order crash . Stop it And not the job continuity
3	3	3	3	3	3	the total
0.75	0.75	0.75	0.75	0.75	0.75	Rate
						The fifth axis (audit procedures in light .of cyber security risks
1	1	1	1	1	1	1. system presence bezel To the effective Internal Censorship Security Risks evaluation on able bank Cyber
1	1	1	1	1	1	2. Cadres Availability bezel Audit system in Eligible mankind . Audit Risks to set on Able Internal
1	1	1	1	1	1	3. system coverage bezel Security For risks Interior Censorship . Audit Her work during Cyber
3	3	3	3	3	3	the total
1	1	1	1	1	1	ateR
						The sixth axis (the professional responsibility of the auditor in light of cybersecurity risks
1	1	1	1	1	1	1. the observer Resurrection bezel procedures By checking accounts . Interior Censorship
1	1	1	1	1	1	2. the observer Resurrection bezel system By checking accounts . Cyber Risks administration
1	1	1	1	1	1	3. the observer Resurrection bezel And analysis By checking accounts Interior Censorship system Reports . Cyber Risks around
1	1	1	1	1	1	4. the observer Resurrection bezel The compliance By checking accounts And policies With strategies bank . Cyber Security Risks administration
1	1	1	1	1	1	5. the observer Resurrection bezel compliance bezel By checking accounts And regulations By legislation The bank Turn organize that And instructions . Cyber Risks
1	1	1	1	1	1	6. the observer Resurrection bezel Disclosure By checking accounts Cyber Risks on The bank administration . Finance Lists in
6	6	6	6	6	6	the total
1	1	1	1	1	1	Rate

By reviewing Table No. (2) above, we note the following:

1 **.**The bank is 100% committed (implemented) to axes (1, 3, 5, 6) above.

2 .The bank is committed (implemented) at a rate of (60%, 75%) to the axes (2, 4) above, respectively.

3 .The bank's commitment to cybersecurity aspects and auditing procedures indicates the existence of an influential relationship between them.

Section Four: Conclusions and Recommendations:

First: Conclusions

Conclusions of the theoretical side- :

This research presents the most important theoretical conclusions reached regarding the results of the cybersecurity risk assessment, which were as follows:

1 -Not obliging the managements of companies (banks) to submit a letter of management acknowledgment of cybersecurity prepared by the General Secretariat of the Council of Ministers. The cybersecurity plan is one of the requirements for protecting financial data. This represents a clear violation on the part of those companies (banks), which entails great responsibility in this regard and risks. Great for everyone.

2 -Ignoring the binding legal aspect in the event that companies (banks) are not obligated to comply with circulars issued for previous years regarding cybersecurity (temporal research sample.(

3 -Failure to oblige the managements of some companies to submit a complete and accurate cybersecurity report will result in that letter losing its importance and thus turning into a mere presumption and not proof of evidence, especially with regard to important elements that lack supporting supporting documents.

4 -The auditor did not pay sufficient attention to cybersecurity risks due to doubts in its preparation, which prevented him from relying on this letter seriously, so the audit process required his effort.

Conclusions of the practical (analytical) side

1 .The bank is 100% committed (implemented) to axes (1, 3, 5, 6) above.

2 . The bank is committed (implemented) at a rate of (60%, 75%) to the axes (2, 4) above, respectively.

3 .The bank's commitment to cybersecurity aspects and auditing procedures indicates the existence of an influential relationship between them.

4 .The basic research hypothesis has been proven, which states (there is an influence relationship between cybersecurity risks and audit procedures.(

Second: Recommendations

1 -The requirements of the Central Bank of Iraq should include a reference to submitting management reports on cybersecurity risks, along with the deadline for submitting financial statement requirements, as well as proposing a law on cybersecurity.

2 -Intensifying efforts towards increasing awareness and educating auditors regarding the importance that the concept of cyber security (and other auditing standards related to electronic auditing) represents to the supervisory opinion submitted, by enrolling them in specialized courses in this field or holding workshops or seminars to ensure that they are helped to practice The profession in its correct form.

3 - The need for the esteemed Accounting and Regulatory Standards Board in the Republic of Iraq to intensify its efforts to issue an (Iraqi) audit guide whose content is based on the international auditing standard for cybersecurity and in a way that is compatible with the local regulatory environment.

4 -The issuances of international accounting standards should be kept up to date in a way that is compatible with the Iraqi environment, taking into account the current developments and openness to foreign investments, with regard to digital transformation and electronic automation, so that it is possible to accommodate local and international requirements and protect them from cyber risks.

5- The necessity of activating the role of the Iraqi Accountants and Auditors Syndicate to carry out its responsibilities in setting international auditing standards for which no audit evidence has been approved in Iraq, related to digital transformation and financial inclusion, to be implemented by auditors' offices and to supervise their implementation on a permanent basis, while holding accountable those who neglect their duties in this regard. Through technical development and openness to the development of the auditing profession.

References:

First – **Arabic references**

Laws, regulations and official documents

1 .Council of Europe Cybercrime Convention 2001

2. Report of the regional profile of the information society in the Arab region for the period 2003-2015 Economic and Social Commission for Western Asia United Nations, Beirut, 2016

3 .Iraqi Electronic Signature and Electronic Transactions Law No. 78, of 2012

4 .Electronic Transactions Law in Jordan of 2001.

5 .COBIT 2019 Government Information and Technology Framework

Books

1 .Lotfy, Amin Al-Sayed Ahmed, International Review and the Globalization of Capital Markets - Alexandria University House 2005

2 .The digital transformation from Earth to space: Opportunities for economic growth or a threat to national security 2022

3 .Salman Abdel Sattar Shaker, "Cybersecurity crimes and the impact of international efforts to combat them," Hattrick Distribution and Publishing, first edition 2023.

4 .Ahmed Sarab Thamer, "Attacks on Computer Networks in International Humanitarian Law," Hattrick Distribution and Publishing, first edition 2023.

5.Al-Sharif Mustafa Kamel, "Cybersecurity Encyclopedia," Dar Al-Qanadeel for Distribution and Publishing, first edition 2024.

6. Muhammad Amin Al-Shawabkeh, Computer and Internet Crimes (Information Crime), third edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2009.

7 .Book on using computers in financial auditing / Dr. Abdulaziz Al-Sayed Mustafa 2021

8 - Talal, Muayyad Ibrahim, "The impact of using the electronic calculator on the work of control and auditing," research submitted for the Higher Diploma in Accounting Control, College of Administration and Economics, University of Baghdad,

Theses, dissertations and research

1 .Makkawi Hassan Imad and Muhammad. “Digital privacy in international law and international conventions.” Journal of Media Research and Studies 20.20 (2022:(

2 .Al-Husseini and Al-Mamouri 2022. Using neural networks to develop the role of an artificial observer in detecting errors

4. Al-Mamouri, Al-Ahmadi (2023) Auditing the comprehensive electronic banking system to detect operational business risks

Second: Foreign references

1. ANTONIA DIN, DIGITAL CONTENT CREATOR, LAST UPDATED ON FEBRUARY 16, 2022, Why Cybersecurity Is Important for Companies?, https://heimdalsecurity.com/blog/why-cybersecurity-is-important-for-companies/ , Last visit on 3-1-2023.

2. Astha Oriel, September 28, 2020, Five Types of Cyber Security for Organizational Safety, https://www.analyticsinsight.net/five-types-cyber-security-organizational-safety/ , Viewed on 3-1-2023.

3. National cyber security centre glossary (2016). Retrieved from https://www.ncsc.gov.uk/information/ncsc-glossary, Viewed on 3-1-2023.

4. Alyoshin, C. П., and O. M. Гайтан. Neural network technology of recognition of hacker applications for traffic interception and analysis= Нейромережева технологія розпізнавання хакерських додатків для переходу та аналізу трафіка. Diss. Чернігівський національний технічний університет, 2020.

5. Ajis, Andri, et al. "The Influence of Transformational Leadership and HRM Practices on Organization Performance: Organization Trust as a Mediator." Budapest International Research and Critics Institute-Journal (BIRCI-Journal) 5.3 (2022): 18474-18487.

6. Al-rimy, Bander Ali Saleh, et al. "Zero-day aware decision fusion-based model for crypto-ransomware early detection." International Journal of Integrated Engineering 10.6 (2018).

7. Cohen, J. "Statistical power analysis for the behavioral sciences (rev. ed.) Lawrence Erlbaum Associates." Inc., Hillsdale, NJ, England (1977).

8. Cooper, D.R. & Schindler, P.S. (2014). Business research methods (12th edn). Boston: McGraw-Hill

9. Ecosip. Dialogues autour de la performance en entreprise: les enjeux. Editions L'Harmattan, 1999.

10. Middleton, Bruce. A history of cyber security attacks: 1980 to present. Auerbach Publications, 2017.