TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 35, 2022

A new decade for social changes

ISSN 2668-7798

www.techniumscience.com

TECHNIUM SOCIAL SCIENCES JOURNAL

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

Auditing cybersecurity risks considering the information renaissance and its impact on the continuity of companies

Asaad Mohammed Ali Wahhab[1], Baneen Hassoun Jawad[2], Emad Hamza Abd Alajeli[3]

[1 2 3]College of Administration and Economics, University of Karbala, Iraq

asaad.m@uokerbala.edu.iq, baneen.hassoon@s.uokerbala.edu.iq, emad.h@s.uokerbala.edu.iq

Abstract. The research aims to identify the role of the external auditor in auditing cybersecurity risks and the size of the cybersecurity risks to which Iraqi companies are exposed and to determine the procedures of the external auditor and Iraqi audit offices in auditing cybersecurity risks and their adequacy, in addition to knowing the impact of cybersecurity risks on the continuity of Iraqi companies. Eighty-five questionnaires were distributed to a sample of external auditors in auditing offices who have experience auditing electronic accounting systems in Iraq, and 77 questionnaires were retrieved from them that are valid for analysis using the SPSS statistical program. There is a relative development in the use of electronic accounting and administrative systems by Iraqi joint stock companies. There is a clear impact on the continuity of companies due to cybersecurity risks that cannot be avoided, as well as the lack of sufficient experience among many work teams in audit offices to audit cybersecurity risks.

Keywords. Audit, cyber security risks, informational renaissance, corporate continuity

1. Introduction

The audit profession today faces significant challenges in the world of big data and the use of electronic and cloud accounting programs, which requires the external auditor and the work team in his office to have experience and skills that enable them to reduce audit risks and express an opinion on financial statements. Cybersecurity risks are among the challenges facing companies. Large companies, especially banks, require internal and external audits, in addition to the management of companies, to develop clear plans and policies to reduce these risks. Auditing cybersecurity risks and their impact on the continuity of Iraqi companies is an urgent need for the Iraqi reality in light of the information revolution, especially in recent times, where Iraq lacks infrastructure and specialists in the field of cybersecurity compared to other countries, this means the importance of working on creating and approving a comprehensive information base for all private and governmental institutions To deal with cyber risks that violate the security stability of corporate information in the world For Iraq, whether, at the level of industrial companies or banks, the literature that dealt with auditing cybersecurity risks and their impact on the continuity of companies was discussed in the first part. In contrast, the second part was devoted to testing and discussing research hypotheses.

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

2. Background

According to Guseva's (2020) study, the growing list of sanctions against Russia can seriously change the situation among the priorities of cyber threats to Russian companies and critical infrastructures. The most advanced methods of protection against potential cyber-attacks should be introduced, considering the imbalance in the company's strategy for business development and between the company's current level of development of existing relationships and methods. Thus local private banking solutions can be entirely successful with adequate protection against cyber threats. At the same time, Sabillon's (2022) study aimed to provide a comprehensive literature review of the most appropriate methods for conducting cybersecurity audits, Auditing scope-specific perspectives and best practices that many of the leading organizations of security and audit professionals provide to follow. In one of the book's chapters, the study reviews the features related to auditing methods and procedures in light of reviewing corporate cybersecurity risks. Rosati et al. l (2022) study indicated that cybersecurity incidents might represent significant risk factors for the quality of financial reports. The study did not find any evidence of security incidents. Cybersecurity leads to lower audit quality, and auditors have increased their awareness of audit risks and established appropriate procedures to deal with the consequences of cybersecurity incidents.

The current study deals with measuring cybersecurity risks audit procedures and their impact on the continuity of companies, which most of the previous studies did not address.

2. Literature Review

2.1 Auditing cyber security risks

As organizations rely heavily on information systems to carry out the production process, the potential risks increase, which means that all organizations are exposed to cyber-attacks. Therefore, cybersecurity risk assessment is about identifying, managing and controlling risks. Risk management is an integral part of any enterprise-level strategy. This article will guide you in performing a cyber risk assessment, reducing costly security incidents, and avoiding compliance issues. Zalata.et.al,(2020)

Certain techniques are used in cyber risk audits to identify and classify risks to organizational processes and assets resulting from using information systems. The main purpose of a risk assessment is to provide a summary to help decision-makers understand the value of the information you are trying to protect. Maldonado& Lobo(2019)

The cybersecurity risk assessment process is a necessary process that must be on an ongoing basis, so the external auditor must devote time and resources to improving security, identifying potential threats, providing a model, or avoiding application interruptions. It must be repeated as new threats emerge and new activities are introduced. Alfraih(2017)

The risks related to cyber security are calculated, and it is the determination of the Probability and impact of these cyber risks if they occur. It all boils down to a simple equation: Impact (if turned on), Probability (to run in the estimated control environment) = Risk rating. Here are some examples of risk assessments: High - There is an urgent threat to the organization, and the risk must be reduced immediately. Medium - The risk reduction must be completed within a reasonable time frame. Low - Threats are normal and generally acceptable. Sakka& Jarboui(2019)

We see that a successful risk assessment process must align with objectives for risk mitigation. Then you can create a risk assessment policy that describes what units should do to monitor their security situation, how to mitigate risks, and what to take or a set of assessment actions.

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

2.2 A conceptual introduction to cyber security

The end of the Cold War brought to light many challenges and threats that the international community had not experienced before, known as asymmetric cross-border or asymmetric threats that do not recognize borders, sovereignty or the idea of the nation-state, which led to transformations in the field of security and strategic studies as well as in political practice. This was accompanied by the technological development of communication, which led to many repercussions due to the emergence of cyber threats and crimes, which became a significant challenge for national and global security - Adiloglu & Gungor (2019). Cyber is the fifth field of war after land, sea, air and space, which necessitated security guarantees. Within this digital environment, it has essentially crystallized in the emergence of Cybersecurity as a new dimension in the field's agenda. From security studies and as a new variable in international relations. Cybersecurity consists of two parts, which we as researchers should highlight as an introduction to determine the importance of Cybersecurity in the new Iraq. Security is the opposite of fear; security is the source of action, i.e. self-confidence. Based on the definition of security policy AKYÜZ (2020), it can be said that security: is the set of rules established by security officers in any place that must be observed by all persons who can Access, which is a broad group concept that includes all operations of entering, exiting, staying or disposing of a place, security in cyberspace contains rules and principles of control of communications, transmission, storage and preservation of information, site security, electronic systems and their investment operations, and communications security. International relation is a term that indicates nothing to threaten rare valuesRamdhani & Arifai (2021)

Cyber is one of the most used terms in the international security dictionary. The etymological approach to the word cyber indicates that it is a Greek word derived from the word cybernetics, meaning the person who directs the ship and is also used figuratively for the controller (the ruler). The term cybersecurity comes from The Arabized word "cyber" from the Latin word "cyber", which recently appeared in English dictionaries, which in Arabic means electronics, which is related to the characteristics and culture of computers and information in addition to technology and virtual reality, as systems, networks and electronic data are considered malicious attacks, Panda. et al. (2019). Cybersecurity deceives network security, information security, application security, the security of processes occurring in networked computers and their ability to retrieve information in the event of a natural disaster or hack. The development of means of communication and information technologies, the transition to the third generation of the information revolution known as the Internet of Things, Zeng et al., (2022) and the increase of cyber-attacks in the information space and its use of electronic weapons such as espionage, viruses, scanning of transmitted data or denial of service, There is an urgent need. A growing need to enact cybersecurity legislation. Cybersecurity is protecting systems, networks and programs from digital attacks that usually aim to access, modify, destroy or extort money from users. Cyber security, also known as technological security (information security or electronic information as defined by Kaspersky), is the practice of defending computers, servers and mobile devices. Kahyaoglu & Caliyurt (2018), and Rosati & Lynn, 2020 define it as a set of measures taken to defend against cyber attacks and their consequences, which include implementing the required countermeasures, which researchers take into consideration (Rosati & Lynn(2020)

2.2.1 Cyber may threaten the national security of countries

(HARE) pointed out that potential threats to the security of states and individuals can exist through cyberspace. Therefore, cybersecurity can be viewed from a national security point

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

of view and then followed by models used to understand patriotism. Security should also apply to Studying cybersecurity issues, HARE, (2010). According to Popescu& Popescu, cybersecurity is taking all necessary measures and precautions that ensure the system's protection to the user so that the security of information and data transmitted by, through or stored is safe. Political systems differ in the content and meaning of protection, and the extent to which rights are preserved and freedoms, and differ in the state's right to intervene, the limits of this intervention and its origins, in the context of maintaining information, information and legal security, as evidenced by the difference, at the level of identifying the actors concerned with regulation and protection, in the Siberian space, and the global system is characterized by its rapid movement that follows transformations internal and external factors multiply, affecting the stability of the administrative and security systems of states, forcing them to improve their abilities to assume their responsibilities and face These shifts and challenges for effective improvement. Popescu& Popescu(2018)

As explained by Pate& Chudasam (2021), there are two ways in which we can respond to threats. The first is the government, which response to cyber threats in legal and regulatory ways, and the second is the private sector's responses - if government responses can be said to be more ad hoc than sector responses. Your replies cannot be ignored. In today's world, the nation's economic power cannot be overlooked as this sector provides it to the government, and its security cannot be quickly seized. Due to the importance of cybersecurity, many countries have made it a top priority, especially after the electronic wars that began to appear between some major countries, a clear sign of the end of the heavy conventional wars. Weapons have been used, and new fights have been announced are electronic wars, and security is characterized by a multidisciplinary social and technical character Rosati & Lynn (2020)

2.2.2 Cyber security challenges in Iraq

The information and technology revolution in the world obliges us to work quickly and efficiently to keep pace with this revolution because whoever loses in this scientific and information race will not only lose his leadership, but he will lose his will. Various security information helps prepare senior political leaders in any country to make sound decisions to manage its political system and protect its national and national interests. This necessarily means working on creating organizations that build on information and its advanced technologies to support the organization in strength with wiser plans and decisions. Jarison & Wilkinson (2018), The presence of the latest technologies in the country requires a specialized team to exploit them. Cybersecurity technology is, to a large extent, the key to the solution to success and solving all the problems of the state. Because security services depend to a large extent on the information they receive and its accuracy, this requires activating the role of information systems and making full use of technology that responds to the changes resulting from various crises, which became a challenge to destabilize the Middle East. Many analysts argue that the wars of the third decade of the twenty-first century will not be wars in the classical sense, with armies fighting on land, at sea, or in the air. Financial information, whether it pertains to companies or individuals, and even countries' economic institutions. Li& Boritz(2020).

It should be noted that most Iraqi institutions outsource the processing of their information from satellites to a service resource outside Iraq's borders, which makes one happy. The information in the servers of these countries, and its return to Iraq, because this procedure constitutes an attack on the security of Iraqi information; in order to avoid such grave violations of the flow of information in the country, Iraq must build an integrated system for information

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

security, so the Iraqi electronic security must constitute the comprehensive legal and regulatory frameworks, and organizational structures, as well as technical means. Furthermore, technology represents the joint efforts of the local and international public and private sectors. It aims to protect the national cyberspace, with an emphasis on ensuring the availability of information systems, enhancing privacy, protecting the confidentiality of personal information and taking all necessary measures. To protect citizens from the dangers of cyberspace. We conclude from the preceding that the challenges facing the concept of cyber security in Iraq are a cause of political instability, recurring turmoil, and different trends between those who take the decision and those who implement it, which means that Iraq needs a thorough study. The reasons for the deterioration of security in general and cybersecurity in particular. Lutfi(2022)

2.2.3 Cyber security and corporate continuity

The information revolution produced three essential elements: information, digital space, and cyberspace. Thanks to the information and Internet revolution, cyberspace has become one of the main elements that affect the international system with its technological tools capable of carrying out mobilization operations. The mobilization of the world and its influence on politics and the different types of power, whether hard or soft. Muslim)2021) The building block of power also shifted from ownership to knowledge and information, which led to an increase in awareness of the importance of technological progress as a basis for gaining power, and from here comes the importance of developing strategic concepts and the advancement of intelligence in the technical, economic, and communication systems fields, and from here comes the impact of cyberspace in transforming the concept of force based on quantity into force based on the result. The misuse of information and communication technologies by terrorists, particularly the Internet and new digital technologies, to commit, incite, recruit, finance or plan terrorist acts is a matter of concern. Increasingly. Member States emphasized the importance of cooperation between the various actors involved. In the face of this threat, including between the Member States and international organizations. In Resolution 2341 of 2017, Askar and Muhammad (2021), the Security Council of Member States, noted the need to: Establish or strengthen national, regional and international partnerships with stakeholders in the public and private sectors, as appropriate, to share information and expertise to prevent terrorist attacks on Critical infrastructure and protection, mitigation, investigation, response and recovery, including through joint training and the use or establishment of appropriate emergency communication and warning networks.

Cyberspace has become part of the international interactions in which the United Nations and the international community seek to control the areas of responsibility, where the rates of threats and opportunities for electronic warfare are increasing dramatically. The conflict has become political with the increase in the number of parties in this region. However, it takes a military form to damage the information wealth of the state's infrastructure and destroy it for political purposes. Al-Otaibi(2021) The dividing line for the world will not be between North and North. The South and the developed and backward world, but on new grounds, the first of which are those who possess cyber power. The ability to make and manage it, on the other hand, those who were denied it although they were allowed to use it, that knowledge and computing have become a significant component of state power, and at the top of its pyramid is a cyber force that affects the national security matrix of any country in Iraq.

The cybersecurity strategy aims to form a coordinated strategy that responds dynamically to national security threats, Al-Ali (2018). The National Cybersecurity Strategy in Iraq aims to manage security threats in cyberspace in line with national security objectives, with

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

the movement of the national cybersecurity vision toward a safe, secure, vibrant and resilient society. Moreover, the trust provides opportunities for its citizens, protects national interests and promotes peaceful interactions and proactive participation in cyberspace for national prosperity. National capabilities in the field of cybersecurity in Iraq towards a coordinated, sustainable and integrated approach to addressing and mitigating risks. Sabah (2016)

Furthermore, reduce cyber risks in cyberspace and protect the national information infrastructure in various fields to raise the cyber level in Iraq towards a secure electronic environment. It also highlights how early warning, detection, interaction and crisis management can be assessed, developed and implemented to provide preparedness for a proactive response. On threats and critical information infrastructure management in Iraq, Iraq ranks 107th globally in cybersecurity and 13th in the Arab world. Several Arab countries have exceeded it to the extent that their financial budgets cannot be compared with Iraq, such as Sudan, Palestine and Jordan. Four countries in the Arab world, namely Saudi Arabia, Oman, Qatar and Egypt, occupied advanced positions in the first quarter. Iraq faced a significant challenge at this level because its youth used these digital platforms. Professionally, the organization faced heroism, courage, professionalism and patriotism. Heavenly (2020).

Continuity is one of the few borrowings on which the accounting theory is based, perhaps the most important of which is accounting and auditing. Any development of the accounting and auditing professions does not conflict with the imposition of continuity. Instead, it reinforces the existence of imposed continuity with the development of the accounting and auditing professions. Civča et al. (2021)

The tax continuity system is one of the most critical accounting loans used in preparing the financial statements in their final form, as the project is supposed to be established in order to complete and continue its work in the foreseeable future and that it will remain and continue for a reasonable and indefinite period. It affects the nature of the enterprise's business that the imposition of continuity in accounting means that the business will continue to operate, will not go out of business, or will not be liquidated. Until this is done, it must be able to increase its resources appropriately. Ali & Flayyih (2021) and (Rydzewska: 2021, 22) indicated that the project would remain and continue for a reasonable period sufficient to use its economic resources according to what is planned and expected and without significant losses to the invested capital using the resources of the social environment for optimal use, without inflicting losses on the rights of society, preserving its external effects and avoiding its external effects.

The imposition of continuity represents the natural expectation of the accounting unit because it reflects the expectations of all parties interested in the business of the economic unit, bearing in mind that the possibility of liquidation or cessation of activity represents a situation.

3.1 Research Importance

He drew the attention of the external auditors to the importance of developing their skills in information security audits, especially cybersecurity, to maintain a high level of performance when issuing their reports, whether about periodic audits or special audits, to express a high-level technical opinion that helps at present. Furthermore, potential investors to make rational decisions about the future of the company's long-term viability.

3.2 Problem of the Research

The research problem lies in asking the following questions: -

1. Is there an impact of the information revolution on breaching cyber security?
2. Does the external auditor in Iraq's audit offices audit Iraq's cybersecurity risks?

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

3. Are Iraqi companies committed to preserving their electronic data from cyber security risks?
4. Does the audit program include sufficiently specialized procedures and auditors to discover company cybersecurity risks?
5. Do cyber security risks affect the continuity of Iraqi companies that use computerized systems?

3.4 Research Aims

T The research seeks to achieve the following objectives: -

1. Identifying the external auditor's role in auditing cyber security risks.
2. B - Identifying the extent of cyber security risks faced by Iraqi companies.
3. Observe the procedures of the external auditor and the Iraqi audit offices in auditing cybersecurity risks and their adequacy.
4. Knowing the impact of cyber security risks on the continuity of Iraqi companies.

3.5 Hypotheses

The research is based on the following main hypotheses:

1. The current information revolution increases cybersecurity risks to Iraqi companies.
2. There is a vital role for the Iraqi audit offices in auditing cybersecurity risks in the companies under audit.
3. Companies must preserve their electronic data from cyber security risks.
4. Audit offices in Iraq seek to develop an appropriate audit program and specialized experts to audit cybersecurity risks for companies subject to audit.
5. Cyber security risks affect the viability of Iraqi companies.

4.1 Cronbach's alpha coefficients

To

Table 1 Cronbach alpha and split-half reliability coefficients to test the stability of the scale

Study variables	Questions No.	Cronbach Alpha
The information renaissance and its impact on cybersecurity risks in Iraqi companies	11	.92
The role of the external auditor in auditing cybersecurity risks	11	.91
The commitment of companies to preserve their electronic data from cybersecurity risks	9	.94
Adequacy of audit programs and experts to face cybersecurity risks in Iraq	7	.92
Cyber security risks and corporate continuity	5	.93
Total	43	.924

Table 1 above shows that the overall reliability coefficient is high, reaching (0.924) for the entire questionnaire and (43) questions. I noted that the questionnaire has high reliability and reliability. The Nanley scale (0.7) was adopted as a minimum reliability scale in field applications.

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

Table 2 The internal consistency of the paragraphs of the questionnaire axes

4.2 Descriptive analysis

Before starting to test the research hypotheses, the researchers verified the data for tracking the normal distribution using the One-Sample Kolmogorov-Smirnov test because this determines the type of tests to be performed and using the Statistical Package for Social Sciences (SPSS) program, the results were as follows:

Table 2 Test the normal distribution of the data for the research variables

One-Sample Kolmogorov-Smirnov Test						
		Axle 1	Axle 2	Axle 3	Axle 4	Axle 5
Normal Parameters[a,b]	**Mean**	3.27627	3.85242	3.64935	4.18615	4.15584
	Std. Deviation	.483400	.320409	.449194	.303359	.353365
Most Extreme Differences	**Absolute**	.101	.119	.095	.213	.251
	Positive	.067	.088	.095	.134	.167
	Negative	-.101	-.119	-.068	-.213	-.251
Kolmogorov-Smirnov Z		.885	1.044	.834	1.869	2.203
Asymp. Sig. (2-tailed)		.414	.225	.490	.184	.122

The results in the table above indicate that the significance of all variables is more significant than 0.05, which means that they follow a normal distribution. Therefore, it is appropriate to conduct parametric statistical tests to verify the validity of the hypotheses.

The five research hypotheses will be tested using the one-sample T-test statistical analysis. The idea of this test is to discover the extent of a significant difference in the mean of the population from which the sample was drawn from a constant value, in addition to the possibility of estimating the confidence period for the mean of the community and the default arithmetic mean of Likert scale will be adopted. The quinquennial and of 3 degrees as a test value to conduct a T-test analysis, and the average answers of the sample members for the five axes of the questionnaire will be used as values to conduct the test using the Statistical Package for Social Sciences SPSS, the results were as follows:

Table 3 Hypothesis test results

Hypothesis number	Sig	T-Table	T Calculated	The decision
1	0.000	1.664	5.015	Acceptance
2	0.000	1.664	23.345	Acceptance
3	0.000	1.664	12.685	Acceptance
4	0.000	1.664	34.311	Acceptance
5	0.000	1.664	28.703	Acceptance

The above table shows that the calculated T value for all hypotheses was more significant than its tabular value at the degree of freedom of 76 (n-1) and that the level of Sig significance was very high and amounted to 0.00, which is less than the accepted error level in social sciences determined in advance by 0.05. The sample data provided convincing evidence to accept the research hypotheses.

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

5. Findings and Discussion

It can be said that the Iraqi (strategic) national security system faces several challenges that can be classified as visible and invisible challenges, the most dangerous of which is manifested in the invisible image that would affect strategic security. (for the individual and the state) This means that these challenges include most governmental and non-governmental sectors and institutions, which revolve around the state's infrastructure to achieve knowledge security for the citizen. Moreover, the challenges faced by official and unofficial state institutions constitute a major challenge to the Iraqi strategic security system; therefore, it has become urgent to focus research and foresight efforts in this area, especially in light of the noticeable increase in challenges facing the system accompanied by similar infrastructure services, aimed at improving conditions The livelihood of individuals by providing them with material and social services, but the country's entry into long wars and international economic sanctions against Iraq, all of which led to its destruction and devastation. Infrastructure

One of the most critical challenges is the weakness of development planning, as planning is one of the main tasks of strategic leadership and an essential element for the stability of the national security apparatus because planning is linked to the future and the use of future sciences and modern scientific theories and methods that contribute to it. Its resources to deter these challenges and achieve the desired goals, and because of the negative repercussions and repercussions that affect the course of work of the strategic institutions of the Iraqi state. Iraq today suffers from a weak strategic planning system, which has negatively affected the work of most of the Iraqi state institutions and their products, which now suffer from weak strategic planning, which represents 'one of the main features of the modern-day economy, and the basis for the work of government institutions in order to achieve the desired national goals. It requires particular abilities to predict and predict the future. In this sensitive period, Iraq needs a planning vision that must solve the financial and security dilemmas that plague the institutional system in Iraq by developing a government program with fixed pillars with planning methods that must be followed to meet Iraq's challenges. The next stage is to think and plan before working through the development of solutions to the problems of the Iraqi state to improve the performance of the strategic system in general in light of the available capabilities.

Through the results of the statistical analysis, the researchers reached some conclusions that can be summarized as follows:

1- There are not enough legal texts in Iraq to monitor cyber security in Iraqi companies.

2- There is a relative development in the use of electronic accounting and administrative systems by Iraqi joint stock companies.

3- The external auditor is essential in auditing the companies' cyber security subject audit.

4- The adequacy of the audit programs of the Iraqi audit offices to audit the cybersecurity risks.

5- The lack of sufficient experience with many work teams in audit offices to audit cybersecurity risks.

6- There is a clear impact on the continuity of companies due to cyber security risks, which cannot be avoided.

7- Most companies have protected electronic programs to ensure the safety of their cyber security.

8- The lack of Iraqi audit offices in the presence of experts specialized in cyber security risks is sufficient to ensure the task's performance with high quality.

Technium Social Sciences Journal
Vol. 35, 18-28, September, 2022
ISSN: 2668-7798
www.techniumscience.com

References

[1] Abdel-Hay, Sabah Abdel-Sabour: (2016) "The use of electronic power in international interactions", Part 2, published research, 2016, Egyptian Institute for Studies, Electronic Library, Available at the following website: https://eipss-eg.org/
[2] Adiloglu, B., & Gungor, N. (2019). The impact of digitalization on the audit profession: a review of Turkish independent audit firms. Journal of Business Economics and Finance, 8(4), 209-214.
[3] AKYÜZ, F., & YEŞİL, T. (2020, October). CYBER SECURITY AND DIGITAL AUDIT. In 1st INTERNATIONAL AUDIT AND ASSURANCE SERVICES (ONLINE) SYMPOSIUM (p. 9).
[4] Alfraih, M. M. (2017). Choosing an external auditor: does the composition of boards of directors matter?" , International Journal of Law and Management.Pp12.
[5] Ali, S. I., & Flayyih, H. H. (2021). The Role of the External Audit in Assessing Continuity of Companies under the Financial Crisis: An Applied Study in the Iraqi Banks Listed in the Iraq Stock Exchange for the Period 2016-2019 El Papel de la Auditoría Externa en la Evaluación de la Continue. 39 (November), 1–20. Estudios de economía aplicada, 39(11), 17
[7] Al-Otaibi. Ziyad bin Muhammad Adi (2021). Cyber crimes are committed via digital media. International Academic Journal of Legal Studies, 3(1), 1-19.
[8] Al-Samawi Muhannad Habib Iraqi digital security...its map, challenges, and future, published article, Nass Channel, 4/21/2020. Available at the following website: https://www.nasnews.com/view.php?cat=29131
[9] Asker, M. p. M., & Mohamed Adel Mohamed. (2021). Putting cyber operations into international law with application to the practice of peacetime espionage. Journal of Legal and Economic Research, 33(1), 257-465.
[10] Civča, D., Atstāja, D., & Koval, V. (2021). Business continuity plan testing methods in an international company. Restrict. Manag. Increase Compet. Trading Co. Latv, 5, Pp 41.
[11] Guseva, Alexey, (2020), "New cyberattacks vectors of Russian critical infrastructure enterprises: Domestic private banking sector view within AI protection methods", Procedia Computer Science, Vol 69, pp.314-319.
[12] HARE, Forrest, (2021), " THE CYBER THREAT TO NATIONA: WHY CAN'T WE AGREE?", Conference on Cyber Conflict, Tallinn, Estonia, pp. 211-225.
[13] Jarison, J., Morris, L., & Wilkinson, C. (2018). The future of cyber security in internal audit. Disponibil online
[14] Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal.
[15] Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. Auditing: A Journal of Practice & Theory, 39(1), 151-171.
[16] Lotfy, Wafaa (2002). International Efforts in Combating Cybercrime Crimes: The Malaysian Experience as a Model. Journal of the College of Economics and Political Science, 23(1), 151-178.
[17] M. Dr. Nibras Ibrahim Muslim. (2021). Cyber-crimes and their impact on cyber security. AL-Qadisiya Journal, 12(1).
[18] Maldonado, I., Pinho, C., & Lobo, C. A. (2019). Determinant factors of external audit opinion modification in Portuguese municipalities. In 2019 14th Iberian Conference on Information Systems and Technologies (CISTI) Pp4
[19] Panda, S., Woods, D. W., Laszka, A., Fielder, A., & Panaousis, E. (2019). Post-incident audits on cyber insurance discounts. Computers & Security, 87, 101593.

[20] Pate, Kathan & Chudasam, Dhaval, (2010), "National Security Threats in Cyberspace", National Journal of Cyber Security Law, Vol 4, No. 1, pp. 12-29.
[21] Perols Rebecca R. & Murthy Uday S. (2021), "The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions" Auditing: A Journal of Practice & Theory, Vol 40, No. 1. Pp. 73-89.
[22] Popescu, C. R. G., & Popescu, G. N. (2018). Risks of cyber-attacks on financial audit activity. The Audit Financiar journal, 16(149), 140-140.
[23] Ramdhani, I., & Arifai, M. K. (2021). AUDIT TATA KELOLA TEKNOLOGI INFORMASI SISTEM INFORMASI MANAJEMEN SEKOLAH DI SMK CYBER MEDIA JAKARTA. Jurnal Ilmu Komputer, 4(2), 38-44.
[24] Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. The International Journal of Accounting, 54(03), 1950013.
[25] Rosati, P., Gogolin, F., & Lynn, T. (2020). Cyber-security incidents and audit quality. European Accounting Review, 1-28.
[26] Rosati, Pierangelo, Gogolin, Fabian, Lynn, Theo, (2020), " Cyber-Security Incidents and Audit Quality", European Accounting Review, Vol 31, No. 3, pp. 701-728.
[27] Rydzewska, A. (2021). Analysis and evaluation of activities aimed at ensuring business continuity by an event industry company in a pandemic situation (Doctoral dissertation, Katedra Systemów Zarządzania). Pp22
[28] Sabillon, Regner (2022), "Research Anthology on Business Aspects of Cybersecurity" Publisher, IGI Global, pp. 77-139. DOI: 10.4018/978-1-6684-3698-1.ch00
[29] Sakka, I. F., & Jarboui, A. (2019). External auditor's characteristics, corporate governance, and audit reporting quality. International Journal of Accounting and Economics Studies, 3(2), Pp24
[30] Thiéry, S., & Fass, D. (2020, July). Cybersecurity risks and situation awareness: Audit committees' appraisal. In International Conference on Applied Human Factors and Ergonomics (pp. 83-87). Springer, Cham.
[31] Zakaria, K. N., Zainal, A., Othman, S. H., & Kassim, M. N. (2019, September). Feature Extraction and Selection Method of Cyber-Attack and Threat Profiling in Cybersecurity Audit. In 2019 International Conference on Cybersecurity (ICoCSec) (pp. 1-6). IEEE.
[32] Zalata, A. M., Elzahar, H., & McLaughlin, C. (2020). External audit quality and firms' credit score. Cogent Business & Management, 7(1).Pp9.
[33] Zeng, J., Wang, X., Liu, J., Chen, Y., Liang, Z., Chua, T. S., & Chua, Z. L. (2022, April). Shade watcher: Recommendation-guided cyber threat analysis using system audit records. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 1567-1567). IEEE Computer Society.