The Impact of Artificial Intelligence and Cyber Security on Audit Quality

Prepared By

Moamen A. Shazly

Assistant Professor of Accounting

Faculty Of Business Studies, Arab Open University, Egypt

Khaled Mohamed Abdelalim

Assistant professor of Accounting, Faculty of political science, Economics and Business Administration, May university in Cairo.

Hesham Zakaria Mohamed

Assistant professor of Accounting, Higher institute of Administrative Sciences in Janaklees, Elbeheira.

Introduction

Artificial Intelligence has been used in computer programs for years and has affected our lives, so to protect this technology we need a strong cyber-security to secure it from cyber threats/incidents thus affect the audit process specially the quality of the audit.

Artificial intelligence is a substitute for human intelligence it is made through equipment and software together to solve complex business problems using reasoning, learning, elucidating, and recognizing same steps same as human expert. AI has expert system instead of expert human and apply machine intelligence instead of human intelligence. Artificial intelligence helps managers in making decisions by providing more precise information, simplifying complex decision factors (Askary, S., et al., 2018, P.332). It is an emerging technology, and it aims to mimic the human judgments and cognitive skills, with competitive advantages for adopters (Munoko, I., et al., 2020, P.1). Also, we can define artificial intelligence as the intelligence exhibited by machines. In computer science, an ideal "Intelligent" machine is a flexible rational agent that perceives its environment and takes actions that increases its chances of success in achieving a goal (Adiloglu et al., 2019, P.2). The Organization for Economic Co-operation and Development (OECD) defines artificial intelligence (AI) as a machine-based system that can make predictions, suggestions, or judgments influencing actual or virtual environments for a certain set of human-specified objectives (Noordin, N. A., et al.,2022, P.1). The usefulness of artificial intelligence is very important concept nowadays in the business and Academic practice. The introduction of the revolution of technology makes changes such as reorganization of industries. Businesses, governments, organizations, and individual's operations are reshaped through artificial intelligence (Issa, H., et al., 2016, P.1).

Cybersecurity provides the required preventive methods to protect data, networks, electronic devices, and servers from malicious attacks and unauthorized access (Naik, B. et al., 2022, P.1). Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Cyber security is a new dimension of risk management.

Recent studies indicate that over the course of only a few years, cyber security has grown to become one of the most important risk challenges facing every type of organization and society. Cybersecurity is more often acknowledged as a severe organizational concern best addressed by integrating it as a part of managerial control system. Cyber security has also become a managerial accounting and auditing matter very much, subject to cost - benefit

analysis, internal control assessment and disclosure policy considerations. The objectives: of cyber security can be divided into three broad categories. First, cybersecurity protects the confidentiality of private information; second, it ensures that authorized users can access information on a timely basis and third, cybersecurity protects the accuracy, reliability and validity of information (Haapamäki, E., et al., 2019, P.2). The American Institute of Certified Public Accountants (AICPA) states, Cybersecurity is one of the most important issues on the minds of management and boards in nearly every company in the world — small and large, private, and public. the AICPA highlights that cyber security is not just an information technology (IT) problem, but also one interested with enterprise risk management problem that requires a global solution (Masoud et al., 2022, P.2). Audit ensures that appropriate policies and procedures have been implemented and are working effectively. So, by implementing AI and Cyber Security in firms, the audit becomes much easier and has better quality than before.

There are two most cited definitions for the audit quality, DE Angelo who defines audit quality as the joint probability that auditors both discover a breach in the client's accounting system and report the breach, and DeFond and Zhang who define higher audit quality as greater assurance of high financial reporting quality (Rajgopal, S., et al., 2021, P.2). Researchers suggest that audit quality is defined as the probability that the auditor will detect a breach and report it. If auditors do not remain independent, they will be less likely to report irregularities, thereby impairing audit quality (Tepalagul, N., & Lin, L. 2015, P.3). Audits are of higher quality at the input level when the people implementing audit tests are competent and independent, and when the testing procedures used can produce reliable and relevant evidence. The quality of audit inputs flows through to the audit process, where audits are of higher quality when the engagement team personnel make good decisions regarding the specific tests to be implemented and appropriately evaluate the evidence from these tests in leading to the audit report (Francis, J. R. 2011, P.2). An Audit Quality (AQ) framework, when appropriately used in an integrated audit offers many benefits to the public because it will provide important information about audit firms with the intention of driving more quality audit services and help investors better evaluate the AQ associated with the financial statements of current and potential investments (Brown, V. L., et,al. ,2016, P.2). Audit quality is fundamental to promote the clean functioning of capital markets. For that reason believed to be compromised due to impaired auditor independence and insufficient utility of expert skepticism (Harber, M., & Marx, B., 2020, P.3)

Audit quality has grown to be a challenge after scandals such as Enron, WorldCom, and Ahold, etc., its research has targeted exceptionally on variations between large five and non-Big five firms (Chen, K. Y., et al., 2005, P.2).

1. Artificial Intelligence (AI)

In the 8th century, time keeping devices were unknown and mysterious to Europeans during that same time frame, however, Muslims already had extensive knowledge about these devices and their inner mechanisms that allowed to show the time accurately, while also mimicking the human behavior in the aspect of understanding and telling time, but in mechanical terms and symbols, all that functioned without the need of any type of human intervention. During that period, the Abbasid Caliphate -at its peak in terms of political and geographical power- was ruled by the Caliph Harūn al-Rashīd, while the Holy Roman Emperor and King of the Franks, Charlemagne, ruled the far west of Germany. The two rulers were in diplomatic contact and exchange delegations and gifts. Harūn al-Rashīd sent a delegation from the city of Baghdad to the court of Charlemagne in the city of Aachen bearing the gift of an elaborate silver water clock. The clock had twelve doors where every hour, one of these doors would open and release its quota of small metal balls equal to the hour. So, if the time is 1 o'clock, the door would open and release one silver ball, and if the time is 2 o'clock, two silver balls are released and so on. Additionally, the balls sounded the number of hours on the clock, so if the time is 5 o'clock, then five balls would be released and fall one after the other, releasing a bass drummed sound effect five times as every time a ball falls on the other, the sound is formed. Also, at 12 o'clock, a mounted horseman appeared and closed all opened doors (McNown, J. S., 1976, P.1).

In the early 17th century, Thomas Hobbes suggested the first idea of Artificial Intelligence (AI) in Europe. He stated that the behavior of a human being could possibly be understood in mechanical terms and symbols. (e.g., numbers, graphs, calculations, and statistics) could be utilized as an equivalent substitute for longer expressions to solve problems. In 1955, Researchers initiated one of the first AI research projects. The goal was to enable machines to use language (in terms of abstraction and concepts) to solve problems and improve itself. Afterwards, Scientists implemented different ways to build up AI. Unfortunately, after the first appeal with the AI research came the “AI Winters” as the research of AI did not accomplish good results because of technology limitations. In modern era, the use of internet has expanded and thus most organizations decided to utilize the use of new technologies. One of these technologies is the Artificial Intelligence (Hussein Issa, et al., 2017, P.3).

Artificial intelligence is defined as a branch of science and computer engineering concerned with the development of intelligent machines or computers capable of thinking, learning, and working independently. The application of artificial intelligence helps to analyze large amounts of data, recognize patterns, and make decisions on its own. There are numerous ways to use AI in Organizations. It can smooth the process of data analysis and the review of documents to help with the decision-making process. In addition, AI can be used to create specific customized reports that meet the organization's needs. It also being used because of the increasing human errors because AI is mainly used to help auditors identify data patterns and make predictions and decisions. Some researchers mentioned that AI is revolutionizing the auditing process and AI enabled auditing software can carry out complex audit much more efficiently, effectively, and accurately than humans is able to. It can also analyze large volumes of data much more quickly and effectively than a human auditor can (Nora Azima Noordin, et al.,2022, P.3).

The Organization for Economic Co-operation and Development (OECD) defines Artificial Intelligence (AI) as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI in the prospective of auditing is machine learning methods used or utilized to represent, structure, model data and large number of unstructured data, leading to more accurate predictions and inference. What separates AI from older data analytics techniques is that AI can copy highly non-linear interrelationships in the data and operation both large volumes of data and unstructured data such as texts and images. AI algorithms can complement other recent technologies, which determine data that can be inspected by AI (e.g., images from drones) or specific applications for AI algorithms (e.g., robotic process automation) (Anastassia Fedyk, et al., July 2022, P.7).

According to some researchers, AI can easily be used in basic missions such as information retrieval from contracts, leases, and invoices. According to the National Association of corporate directors, directors rate AI as the biggest technology disruptors yet also regard it as the biggest business enabler likely to aid their organizations in the next 12 months. Given current advances in AI and machine learning, it should be obvious that an AI-based application can perform the work of Audit Committees members (AC) (Dheeriya, P., & Singhvi, M., 2021, P.7).

Few Companies have already started to utilize the potential of AI to help improve the auditing process. Etisalat, for example, has started using AI to help with customer service, and companies such as PricewaterhouseCoopers (PwC)

are using it with auditing and compliance. Companies that use AI in auditing do so by various techniques. One of which is called "Cognitive Auditing", which is a term used to describe a computerized process that uses AI to increase audit quality by helping auditors find errors and issues in financial reports faster. However, some drawbacks might surface because of using AI. For instance, one study concluded that 95% of accountants risk losing their jobs due to the development of new machine technology. Additionally, companies may no longer need human auditors to audit their books as AI has started to become more efficient at discovering errors and abnormalities in financial data. This could result in significant job losses in both the accounting and auditing sectors and thus may lower the quality of financial audits. On the other hand, most organizations have realized that the potential of using AI to significantly decrease the need for human auditors is so tremendous that these firms have weighted this potential to be much more significant than the drawbacks that come with such system. One Researcher suggested that if organizations prefer using AI in their businesses, they should not neglect potential threats caused by AI on financial data. As AI becomes more proficient in identifying data patterns, it may also be able to identify sensitive information that should not be disclosed to outsiders. If this information fell into the wrong hands, it could be used to manipulate financial institutions or to commit other crimes (Azima, et al., 2022).

2. Cyber security

It is important to organize information risk and is naturally obtained through the application of assurance activities. The UK government's national technical authority for information assurance (CESG) has explained assurance as means of providing independent confidence that security controls are operating the functions expected from them. According to the National Institute of Standards and Technology (NIST) defines cybersecurity as a process of protecting information by prohibiting, detecting, and responding to cyber threats. The complication of cyber-security especially, it comes less than from the devices we use than from the people behind them. The National Initiative for Cyber-security Career and Studies defines cyber-security within its dictionary as the activity or process, ability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation (Kahyaoglu, S. B., & Caliyurt, K.2018, P.3).

Cyber-security was mainly created to prevent cyber threats/incidents. Cyber-security incidents are vastly increasing every year because of the use of internet, cloud computing, and mobile devices. Cyber-security incidents are

complicated and contain diverse occurrences. For instance, Equifax, a credit reporting agency, admitted on 7th of September 2017, that hackers had compromised information of over 140 million individuals between May and July of the same year. Hackers were able to expose vulnerabilities of their website and gained access to social security numbers, birth dates, driving license numbers, and credit numbers information. The after effects of the breach were material. The firm stock price dropped approximately 18% upon first disclosure of the breach. Court documents filed in the settlement of the case suggest that the minimal cost would be 1.38 billion USD. Number of observational studies concluded that cyber-securities incidents typically result in a serious damage to the affected firms in terms of a loss in the market value, remediation cost, fines, and reputation (Pierangelo Rosati et al.,2020, P.5).

The American Institute of Certified Public Accountants (AICPA) stated that Cybersecurity is one of the top issues on the minds of management and boards in nearly every company in the world—large and small, public, and private. Therefore, it is important that every organization at least consider a cybersecurity risk management program. In addition, certain organizations and their stakeholders need timely, useful information about organizations' cybersecurity risk management efforts (Elina Haapamäki, Jukka Sihvonen, 2019, P.4).

To protect its customer's valuable information, A firm should acquire an effective internal control with a powerful cyber-security. Organizations face various types of risks with threat landscape growing every day.

To reduce these risks, The American Institute of Certified Public Accountant (AICPA) issued a new framework to reinforce Cyber-security risk management which aims to help businesses meet the growing challenge created by cyber threats. (Islam, M. S., et al., 2018, P.6).

This research suggests that one way to combat these potential threats is by implementing a strong Cyber-Security. The AICPA issued a new framework for Cyber-Security risk management to help businesses deal with the growing challenges caused by Cyber-Threats /incidents. One result of this new framework is the surfacing of a new type of management called Enterprise risk management (ERM), which took a responsibility upon itself to be the ones watching over the constant growth caused by corporate uncertainty and financial scandals, while also keeping levels of these factors in check. Additionally, the (ERM) is implemented to improve audit quality by acting as a process that is applied in strategy settings across the organization and is affected by that organization's board of directors, management, and other personnel, in order to discover potential events that may in turn influence the firm, manage risk to be

within its moderate levels, and provide reasonable assurance regarding the achieved goals of company's objectives, thus improving the quality of an audit (Md. Islam, et al., 2018, P.6).

The number and severity of cyber threats have been uncommon in recent years, and successful cyber-attacks have been reported regularly. Moreover, the costs of cyber-attacks are terrific; therefore, cybersecurity risk management is debated to be exceptionally important for organizations. In relation to this, Hausken asserted that the intensity of cyber war has increased through the internet revolution. Relatedly, suggested that the internet revolution has dramatically changed the way in which individuals, firms, and the government communicate and conduct business (Elina Haapamäki, Jukka Sihvonen, 2019, P.4).

Although, Cyber-security proved its worth for most organizations, some members of the board still don't possess a deep understanding for this system. For example, a recent study of more than 250 board members was conducted. The study concluded that cyber-security is a rising concern, even exceeding compliance risk, and approximately 74% of board directors indicated that their CEOs have a strong knowledge of regulatory compliance risks, while only 51% stated that their CEOs possess a substantial understanding of Cyber-security topics (Md. Shariful Islam et al., 2018, P.8).

3. Audit Quality

All previous points discussed (AI & Cyber-Security) are looked at as factors that are used in our paper to affect audit quality. But what is Audit Quality? Auditing standards have stated that the concept of audit quality is based on the issuance of "appropriate" audit report on the client's compliance with generally accepted accounting principles (GAAP). Although this is the concept viewed by auditing standards, audit quality is a much more complex concept that cannot be reduced to a simple definition. For instance, the legal view of auditing provides two types of audit quality that contrast each other: "audit failure" and "non-audit failure".

An audit failure happens in the case of lack of auditor independence, or if the auditor independence is present, but the auditor incorrectly issues an unqualified audit report due to failure to accumulate sufficient competent evidence as necessitated by auditing standards. On the other hand, a "good audit" or a non-failure audit is one in which the auditor complies with auditing standards and issues the accurate opinion about the client's financial statements at a reasonable level of audit risk (Francis, J. R., 2011, P.3).

These two components are what define the types of audit quality in general. Between these two types, the SEC, according to evidence obtained from litigation, pointed out that the rate of audit failure is very low. This could be the case, however, because it is likely that that rate is higher, mainly as result of SEC's insufficient resources to track all cases and determine the levels of each firm's audit quality. As a result, it is quite possible that there are many low-quality audits that are so low, that it is nearly as identical as an audit failure, and this why it is crucial to think about the concept of audit quality as a spectrum that ranges from very low audit quality to very high quality, so one could be able to identify the many similarities between a very low audit quality, and an audit failure (Francis, J. R., 2011, P.4).

Another Common definition of Audit Quality is that it is a process that an auditor goes through to evaluate a financial statement's risk level of a material misstatement. In other words, an auditor inspects whether a financial statement has been fairly documented to ensure that there are no material misstatements and to ensure a strong internal control. In these conditions auditor's independence is a critical point when reporting errors or fraud. Find and report material errors, dependents on different factors related to auditors' competencies. Training and experience prepare the auditor for the discovery of material misstatements. Moreover, independence would be the circumstance to report what has been discovered (Hosseinniakani, S. M., et al., 2014, P.2).

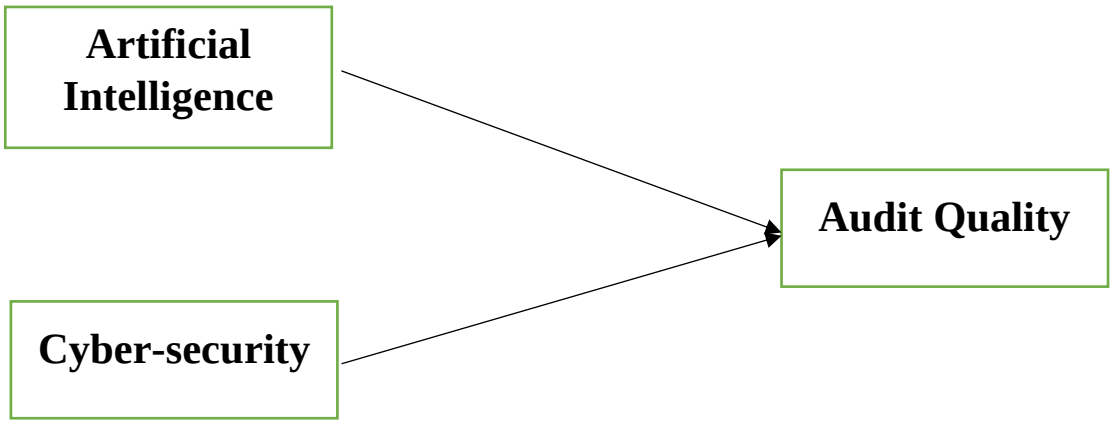
In this instance, Greater perceived audit quality can lead to improvements in audited clients' investment processes. In terms of achieving reasonable assurance, it can be said that audit quality refers to how well the auditing process can identify and report material inaccuracies in the financial statements (Hosseinniakani, S. M., et al., 2014, P.2).

From the client's perspective, the important thing is to improve the audit process and quality report. Due to the wealth function of the firm, shareholders are more interested in getting high quality audit reports, whereby preferred higher quality audit. Stakeholders are also concerned about audit quality. Accordingly, the lack of the audit quality may decrease the probability of discovering an audit failure (Hosseinniakani, S. M., et al., 2014, P.2).

All in all, an audit quality is a systematic approach which is put together for an auditor to carry out a thorough examination of accounts and detect possible errors or anomalies, and the auditor's willingness to provide an objective opinion on these examined items. This systematic approach is made up of several attributes such as "professional judgement", which is an important attribute because it greatly enhances the informational value of auditing for external users (Arruñada, B., 2000, P.4).

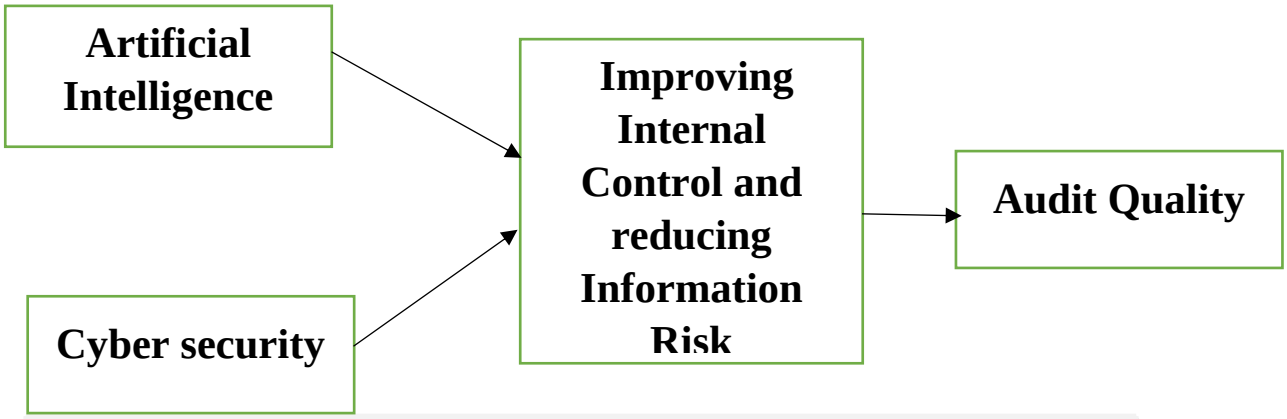
. For instance, in the presence of internal control deficiency, such as an increase in inherent and control risk, auditors may increase their sufficient testing to maintain similar levels of audit quality. As a result, auditor's concentrated efforts and sufficient testing can neutralize the effects of Cyber-Threats / Incidents on Audit Quality (Rosati, et al., 2020, P.5).

4. Impact of Artificial Intelligence and Cyber Security on Audit Quality



As AI becomes more proficient in identifying data patterns, it may also be able to identify sensitive information that should not be disclosed to outsiders. If this information fell into the wrong hands, it could be used to manipulate financial institutions or to commit other crimes.

Cyber security provides the required preventive methods to protect data, networks electronic devices, and servers from malicious attacks and unauthorized access. The objectives of cyber security can be divided into three broad categories. First, protects the confidentiality of private information; second, ensures that authorized users can access information on a timely basis and third, protects the accuracy, reliability and validity of information. So, AI is a powerful technology that can improve cyber-security by preventing new attacks using autonomous systems and learning patterns.



Using AI and Cyber-security are improving the internal control and reducing information risk by protecting information from threats on the internet. AI reduces human errors, increases accuracy, and protects firms against unknown threats and learns its patterns, while Cyber Security protects firms' information against known cyber threats, which directly improve audit quality through auditor's willingness to provide an objective opinion.

5. References

1. 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.
2. Albitar, K., Gerged, A. M., Kikhia, H., & Hussainey, K. (2020). Auditing in times of social distancing: The effect of COVID-19 on auditing quality. International Journal of Accounting & Information Management.
3. Arruñada, B. (2000). Audit quality: attributes, private safeguards, and the role of regulation. European Accounting Review, 9(2), 205-224.
4. Askary, S., Abu-Ghazaleh, N., & Tahat, Y. A. (2018, October). Artificial intelligence and reliability of accounting information. In Conference on e-Business, e-Services and e-Society (pp. 315-324). Springer, Cham.
5. Brown, V. L., Gissel, J. L., & Neely, D. G. (2016). Audit quality indicators: perceptions of junior-level auditors. Managerial Auditing Journal.
6. Chen, K. Y., Lin, K. L., & Zhou, J. (2005). Audit quality and earnings management for Taiwan IPO firms. Managerial Auditing Journal.
7. Dheeriya, P., & Singhvi, M. (2021). A CONCEPTUAL FRAMEWORK FOR REPLACING AUDIT COMMITTEES WITH ARTIFICIAL INTELLIGENCE INFUSED BOT. EDPACS, 63(3), 1-18.
8. Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process? Review of Accounting Studies, 27(3), 938-985.
9. Francis, J. R. (2011). A framework for understanding and researching audit quality. Auditing: A journal of practice & theory, 30(2), 125-152.
10. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808-834.
11. Harber, M., & Marx, B. (2020). Audit quality and independence concerns in the South African audit industry: Contrasting views. South African Journal of Accounting Research, 34(1), 1-23.
12. Hosseinniakani, S. M., Inacio, H., & Mota, R. (2014). A review on audit quality factors. International Journal of Academic Research in Accounting, Finance and Management Sciences, 4(2), 243-254.
13. Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. Managerial Auditing Journal.

14. Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. Journal of Emerging Technologies in Accounting, 13(2), 1-20.
15. Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. Managerial Auditing Journal.
16. Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. Research in Economics, 76(2), 131-140.
17. McNown, J. S. (1976). When time flowed The Story of the Clepsydra. La Houille Blanche, (5), 347-353.
18. Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. Journal of Business Ethics, 167(2), 209-234.
19. Naik, B., Mehta, A., Yagnik, H., & Shah, M. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems, 8(2), 1763-1780.
20. Noordin, N. A., Hussainey, K., & Hayek, A. F. (2022). The use of artificial intelligence and audit quality: An analysis from the perspectives of external auditors in the UAE. Journal of Risk and Financial Management, 15(8), 339.
21. Rajgopal, S., Srinivasan, S., & Zheng, X. (2021). Measuring audit quality. Review of Accounting Studies, 26(2), 559-619.
22. Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. European Accounting Review, 31(3), 701-728.
23. Tepalagul, N., & Lin, L. (2015). Auditor independence and audit quality: A literature review. Journal of Accounting, Auditing & Finance, 30(1), 101-121.
24. Yebi, D. K., & Cudjoe, E. K. (2022). Artificial Intelligence as a Disruptive Business Model in Auditing. A study of the impact of artificial intelligence on auditors' skills and competence, audit process, and audit quality.'