International Journal of Research in Finance and Management

P-ISSN: 2617-5754
E-ISSN: 2617-5762
IJRFM 2024; 7(2): 125-132
www.allfinancejournal.com
Received: 08-05-2024
Accepted: 17-06-2024

Ali Abdul Hussein Raj
Department of Banking and Financial Sciences, Faculty of Administration and Economics, Al-Qadisiyah University, Iraq

Ali Hilal Union
Department of Accounting, Faculty of Administration and Economics, University of Kufa, Iraq

Ameer Saheb Shaker
Department of Accounting, Faculty of Administration and Economics, University of Kufa, Iraq

Correspondence
Ali Abdul Hussein Raj
Department of Banking and Financial Sciences, Faculty of Administration and Economics, Al-Qadisiyah University, Iraq

Cyber auditing: Protecting data in the digital age

Ali Abdul Hussein Raj, Ali Hilal Union and Ameer Saheb Shaker

DOI: https://doi.org/10.33545/26175754.2024.v7.i2b.353

Abstract
The current study aimed to identify the concept of cyber auditing through research into data protection in the digital age. The study followed the descriptive analytical approach in applying the study in Iraq to a number of 100 specialists and experts in the fields of cyber auditing and cyber security. The study concluded that the most important obstacle to cyber auditing is that the lack of clarity of roles and responsibilities between cyber audit teams and other departments affects efficiency. The most important result of enhancing cyber auditing techniques was that the use of advanced data analysis tools helps detect cyber threats faster. The role of advanced technologies in cyber auditing is that they allow advanced data analytics to detect patterns of anomalous behavior and potential threats. One of the most important expenses and costs associated with cyber auditing is that the need to train and develop the technical skills of the cyber audit team increases costs. The most important results of evaluating the impact of cyber auditing on data security and business continuity were that implementing cyber auditing on a regular basis improves the level of organizational data security.

Keywords: Cyber audit, data security, data analytics, artificial intelligence

Introduction
Today's world is undergoing immense change, with information technology serving as the primary instrument and force impacting the contexts in which enterprises function. The rate of technological change in the manufacturing and service sectors has accelerated dramatically during the previous two decades. This implies that information technology gives potential for innovations and improvements in many industries in which it may be applied, since it has played a significant role in creating and enhancing the performance of numerous businesses, whether production or service (Whitman & Mattord, 2018) [4].

Both have a role, and as a result, many different government agencies have invested in and benefited from these advancements to increase performance. Security is regarded as the essential underpinning of civilization, and it is hard to conceive the expansion of any activity without obtaining it, whether at the technological or legal levels. With the emergence of the information society and cyberspace, security has turned into one of the services sector, which constitutes an added value and a basic pillar for the activities of governments and individuals alike, such as applications for e-government, e-health, and distance education (Rittinghouse & Hancock, 2017) [3].

Inquiry, e-commerce, and so forth. However, the many faces of cybersecurity, and its dangerous repercussions that go beyond harming individuals and institutions to endangering the safety of states and governments, make the task of those in charge of the subject more complex and difficult, and require a comprehensive and integrated approach to all of the challenges presented by cyberspace (Pathak, 2015) [2].

So that the responses and proposed solutions are effective and effective. Achieving security and building confidence in cyberspace are among the basics of harnessing information and communications technologies in the fields of development to serve human societies (Kearns, 2016) [1].

Study Problem
The information security of countries and institutions today is exposed to many risks, the most important of which are attempts to penetrate databases and reveal highly confidential information, including cyber penetration that poses harm to institutions. Hence, the problem

lies in how to achieve institutional information security.

Research importance

This study helps to increase awareness of the value of cyber protection and offers useful suggestions for improving digital security in contemporary settings.

Study Questions

1. What are the primary obstacles that today's institutions and companies face while conducting cyber audits?
2. Given the changing nature of cyber risks, how may cyber audit techniques be strengthened to achieve greater data security?
3. How can cutting-edge cyber technologies like data analytics and artificial intelligence improve cyber audits?
4. What are the financial and technological expenses related to conducting cyber audits, and what steps might be taken to increase their effectiveness?
5. How can the impact of cyber audit techniques on data security and business continuity be evaluated, as well as how successful are they?

Study Objectives

1. Determine whether cyber threats influence enterprises and how data security is impacted by them.
2. Provide a strong foundation for cyber audits to improve data security and address evolving threats.
3. Examine the ways in which cyber audit operations may be improved and made more efficient via the use of technologies like data analytics and artificial intelligence.
4. Provide inventive and useful suggestions on how businesses may strengthen cyber verification and data protection.
5. Analyze how applicable cyber audit techniques affect data security and business continuity.

Study limits

- **Time limits:** In order to account for contemporary cyber risks and technical advancements, the research concentrates on the years 2024 and beyond.
- **Spatial Boundaries:** Using Iraq as a case study, the study focuses on identifying regional obstacles and solutions for cyber and data security assessments.
- **Limitations on the research's objectives:** In the context of Iraq, the study aims to attain high objectivity by offering a thorough and impartial examination of the problems and solutions pertaining to data security and cyber auditing applications.

Study Concepts

- Cybersecurity auditing is the practice of assessing and managing data security in order to find and fix security flaws.
- Cybersecurity refers to a collection of methods and tools used to defend networks and systems from online attacks.
- **Cyber threats:** Perils and assaults that jeopardize the safety of information and digital infrastructure.
- **Artificial intelligence:** Using artificial intelligence approaches to improve threat detection and security response in cybersecurity, or AI in cybersecurity.

Theoretical Framework

Study by Maryam Hussein (2013) [5], the study's goal is to provide a complete framework for e-government and the use of information technology tools in various organizations, as well as to offer an introduction presentation of the idea and promote awareness and interest in it. The study's problem is that the implementation of e-government in many government agencies and ministries in many countries has resulted in an important problem: The intellectual absorption of this concept by workers in government agencies and citizens, the lack of legislation and laws regulating electronic transactions, and the lack of an electronic signature regulating electronic transactions. The study found that the implementation of e-government necessitates the restructuring of departments to meet e-government standards, as well as the qualification and training of staff on e-government applications. Governments that utilize the e-government application must also produce proper legal regulations for the use of e-government and implement an electronic signature to ensure that books are approved. The official nature, in addition to the necessity to investigate the barriers to e-government implementation in the experiences of developed and developing nations, as well as a lack of understanding among certain people and workers about the idea and its significance. Among the most important recommendations were: investigating the importance of adapting the requirements of e-government to the requirements of change and compatible with the applications of e-government projects, and the creation of The necessary plans to qualify and train employees in a way that is compatible with the use of modern technologies and apply the electronic government method, including programs to protect citizens' data and information in all transactions by establishing the necessary legal legislation and implementing electronic signatures. In addition, before beginning to undertake this project, read about the experiences of industrialized countries. Furthermore, developing countries have challenges that might lead the initiative to fail.

Study by Imad Ahmed Abu Shanab (2012) [6], “This book deals with e-government projects between theory and practice” in 2010, where e-government projects and initiatives were reviewed, through a group of chapters that reviewed the basic principles, definitions and elements, and the steps that are followed to implement these projects. The economics and methods of evaluating these projects were also reviewed, And modern trends in scientific research in this field. Information security and systems architecture were also reviewed as topics that are predominantly technical and administrative in nature. The phenomenon of e-government belongs, from a scientific and literary standpoint, to a group of fields, including: public administration, political science, information technology, and business administration. Accordingly, and given the importance of the topic from an administrative perspective, it highlights the role of e-government in activating community development, popular participation, and the democratic process. The focus is on two main axes: e-management and community development, which are two

important axes that fall under the umbrella of e-government. The book was divided into eight main chapters. The first chapter dealt with the subject of e-government in general, then five chapters dealt with various topics in electronic administration, and two chapters dealt with community development and the digital divide. The recent events in the Arab world make it important to raise such issues so that governments and the public sector do not remain isolated from the popular movement, and so that information technology can be used to consolidate trust between governments and individuals.

Study of Al-Arabi Attia (2012) [7], The problem in this study lies in (what is the impact of the use of information technology on the job performance of workers in local government agencies). Among the results of the study was the existence of a statistically significant relationship between the use of information technology and the job performance of employees, which confirms the importance of working and taking positive steps in investment and development in This tool is in addition to the existence of a statistically significant relationship between the use of information technology and (volume of performance, quality of performance, efficiency of performance, simplification of work), and the most important proposals that the researcher arrived at are: working to define the goal of the administrative apparatus in light of global changes and reconsidering some Administrative structures in line with the expected role of the administrative apparatus, achieving balance between the units of the administrative apparatus and its affiliated departments, reconsidering similar functions that fall within the same single department, ensuring coordination between different activities and units to prevent conflicts of specialization or duplication of work, activating the role of follow-up and evaluation units, and harmonizing the Efficiency and the social dimension, working to modernize and develop the information technology infrastructure on a permanent and continuous basis, commensurate with the nature of work, as well as internal computer connectivity between administrative departments so that speed in providing information and integration in providing services is achieved, preparing programs and training courses, and holding appropriate workshops and seminars for various administrative levels. About effective ways to deal with information technology, and working to provide this tool for completing work in order to increase speed and accuracy in completing tasks and duties.

Methodology

The study relied on the descriptive analytical method, as it is one of the most widely used methods in social and human studies, which includes the use of field survey methods to collect data using a questionnaire and analyze it.

Study population

The study population includes specialists and experts in the fields of cyber auditing and cyber security, including specialists in information technology, cyber security, cyber incident response, cyber data analytics, and other related disciplines.

The study sample

Sample size: The study targets a sample of 100 individuals.

Selection: The sample is appropriately selected to ensure balanced representation of various groups and expertise related to cyber auditing, including public and private institutions, academic and industry experts.

Distribution methods: Electronic questionnaires were used to collect data from sample members.

Analysis of the results

Part 1: Demographic data

Table 1: Gender

Gender	Frequency	Percentage
Male	54	54
Female	46	46
Total	100	100

The data show that the total frequency of the study was 100 people, with males representing 54% of the sample percentage, while females representing 46%. This distribution shows a clear difference in sexual representation within the studied sample.

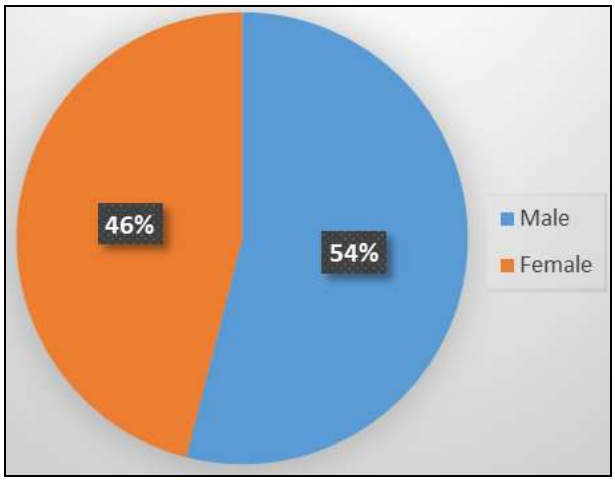

Fig 1: Gender

Table 2: Age

Age	Frequency	Percentage
Less than 25	18	18
25-35	54	54
36-45	21	21
More than 45	7	7
Total	100	100

The data shows that the studied sample consists of 100 people, 12% of whom are under 25 years old, while the age group between 25 and 35 years represents 29%. In addition, the age group between 36 and 45 years represents 21% of the sample, while the proportion of people over the age of 45 years is 7%. These results show the distribution of ages within the sample and the variation in age representation between different groups.

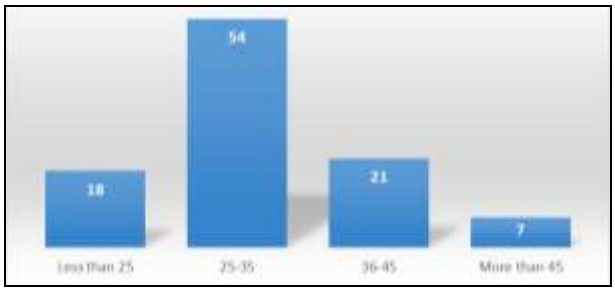

Fig 2: Age

Table 3: Qualification

Qualification	Frequency	Percentage
High school and below	11	11
Diploma	16	16
Bachelor's	42	42
Master's	19	19
Ph.D	23	23
Total	100	100

The results of the study show a diverse distribution of qualifications among the participants, with bachelor's holders representing the largest percentage, at 57%, followed by doctoral holders, at 15%. While the diploma represents 11%, the master's degree represents 17%, while the secondary school and below represents 6% of the sample.

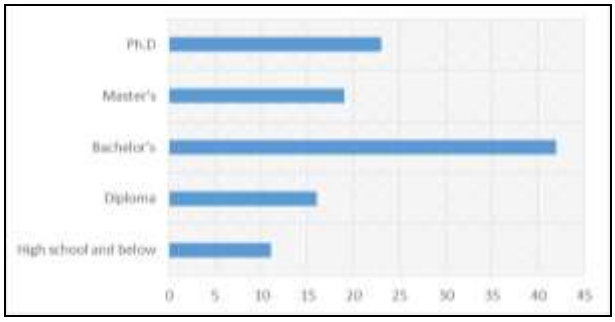

Fig 3: Qualification

Part 2: Topics of the study

The first axis: Basic obstacles to cyber auditing

	Phrase	Mean	Standard Deviation
1	The complexity of an organization's technological infrastructure poses a challenge to cyber auditing.	3.66	1.35
2	The lack of qualified human resources in the field of cyber auditing hinders the effective implementation of operations.	4.12	1.02
3	Lack of clarity of roles and responsibilities between cyber audit teams and other departments affects efficiency.	4.31	0.93
4	The absence of senior management support to invest in cyber auditing limits an organization's ability to adapt.	3.80	1.07
5	Difficulty determining the scope and limits of cyber auditing due to the changing nature of risks.	4.24	0.90

The most important basic obstacles to cyber auditing are that the lack of clarity of roles and responsibilities between cyber audit teams and other departments affects efficiency, with an average of 4.31. Secondly, the difficulty of determining the scope and limits of cyber auditing due to the changing nature of risks, with an average of 4.24. Thirdly, the lack of qualified human resources in the field of cyber auditing. It hinders the effective implementation of operations with an average score of 4.12.

The second axis: Enhancing cyber auditing techniques

	Phrase	Mean	Standard Deviation
1	Using advanced data analysis tools helps detect cyber threats faster.	4.68	0.60
2	Developing continuous monitoring programs for cyber activities enhances audit and response capabilities.	4.48	0.83
3	Adopting artificial intelligence techniques to analyse records and data improves the accuracy of audits.	4.10	1.02
4	Implementing data encryption mechanisms and regular backups increases the security of institutional data.	4.01	0.83
5	The use of standardized audit frameworks and protocols contributes to standardizing practices and improving effectiveness.	4.04	1.00

The most important results of enhancing cyber auditing techniques were that using advanced data analysis tools helps detect cyber threats faster, with an average of 4.68. Also, developing continuous monitoring programs for cyber activities enhances audit and response capabilities with an average of 4.48. Thirdly, adopting artificial intelligence techniques to analyze records and data improves the accuracy of audits by an average of 4.10.

The third axis: The role of advanced technologies in cyber auditing

	Phrase	Mean	Standard Deviation
1	Advanced data analytics enables detection of anomalous behaviour patterns and potential threats.	3.88	1.06
2	Artificial intelligence applications help predict and respond better to cyber	3.68	1.21

	risks.		
3	Automating audit and review processes using robots increases the efficiency and speed of audit procedures.	3.34	1.31
4	Using machine learning techniques to monitor and analyse data improves an audit's ability to detect breaches.	3.62	1.19
5	Integrating advanced cybersecurity technologies such as Blockchain enhances the integrity and security of data during audits.	3.69	1.10

The role of advanced technologies in cyber auditing is that they allow advanced data analytics to detect patterns of anomalous behavior and potential threats, as it came with an average of 3.88. Incorporating advanced cybersecurity technologies such as Blockchain also enhances data integrity and security during audits with an average of 3.69. AI applications also help better predict and respond to cyber risks, with an average score of 3.68.

Fourth axis: Expenses and costs associated with a cyber-audit

	Phrase	Mean	Standard Deviation
1	Investing the necessary resources in technology infrastructure is essential to effectively implement a cyber-audit.	3.66	1.35
2	Employing specialized competencies in the field of cyber auditing requires significant additional costs.	4.12	1.02
3	The need to train and develop the technical skills of the cyber audit team increases costs.	4.31	0.93
4	Acquiring advanced cyber auditing tools and systems requires significant financial investments.	3.80	1.07
5	Covering cybersecurity and risk insurance costs is vital but expensive.	4.24	0.90

The most important expenses and costs associated with cyber auditing are that the need to train and develop the technical skills of the cyber audit team increases costs by an average of 4.31. Covering cybersecurity and risk insurance costs is vital but expensive, with an average of 4.24.
Also, employing specialized competencies in the field of cyber auditing requires large additional costs with an average of 4.12.

Fifth axis: Evaluate the impact of electronic auditing on data security and business continuity

	Phrase	Mean	Standard Deviation
1	Implementing cyber auditing on a regular basis improves the level of organizational data security.	4.00	0.80
2	Electronic audit procedures contribute to early detection of cyber threats.	4.00	1.00
3	Cyber audit results help develop continuity and disaster recovery plans.	3.90	1.10
4	Reports and analyses resulting from a cyber-audit increase management's awareness of risks.	3.70	1.20
5	Implementing cyber audit recommendations improves the ability to confront cyber-attacks.	3.60	1.20

The most important results of evaluating the impact of cyber auditing on data security and business continuity were that implementing cyber auditing on a regular basis improves the level of organizational data security with an average of 4.00. Electronic audit procedures also contribute to early detection of cyber threats, with an average of 4.00. Cyber audit results also help in developing continuity and disaster recovery plans, with an average of 3.90.

Discussion

The results of the current study agreed with the study (Hussein, 2013) [5] in that the most basic obstacles to cyber auditing are that the lack of clarity of roles and responsibilities between cyber audit teams and other departments affects efficiency and the difficulty of determining the scope and limits of cyber auditing due to the changing nature of risks, as well as the lack of qualified human resources. In the field of cyber auditing hampers the effective implementation of operations.
The current study agreed with the study of (Abu Shanab, 2012) [6] in that enhancing cyber auditing techniques is that the use of advanced data analysis tools helps detect cyber threats faster. Also developing continuous monitoring programs for cyber activities enhances audit and response capabilities. Third, adopting artificial intelligence techniques to analyze records and data improves the accuracy of audits.
The results of the current study agreed with the study (Attia, 2012) [7] in that the role of advanced technologies in cyber auditing is that they allow advanced data analyzes to discover patterns of abnormal behavior and potential threats, as it came. Incorporating advanced cybersecurity technologies such as Blockchain also enhances data integrity and security during audits with an average of 3.69. AI applications also help better predict and respond to cyber risks.
The results of the study agreed with the study of (Kearns, 2016) [1]. The most important expenses and costs associated with cyber auditing are that the need to train and develop the technical skills of the cyber audit team increases costs. Covering cybersecurity and risk insurance costs is vital but expensive. Also, employing specialized competencies in the

field of cyber auditing requires significant additional costs.

Conclusion

The most significant challenges to cyber auditing are the lack of clarity of roles and responsibilities between cyber audit teams and other departments, the difficulty of determining the scope and limits of cyber auditing due to the changing nature of risks, and the lack of qualified human resources in the field of cyber auditing, which impedes the effective implementation of operations.

Enhancing cyber audit processes by utilizing modern data analysis technologies to spot cyber risks faster. Additionally, having continuous monitoring procedures for cyber activity improves audit and reaction capabilities. Third, using artificial intelligence to examine records and data increases audit accuracy.

The function of sophisticated technology in cyber auditing is to enable advanced data analytics to discover patterns of aberrant activity and possible dangers. Using modern cybersecurity technologies such as Blockchain improves data integrity and security during audits. AI applications also aid in the prediction and response to cyber dangers.

The most significant expenditure and cost involved with a cyber-audit is the cost of training and developing the technical capabilities of the cyber audit team. Covering cybersecurity and risk insurance expenses is necessary but costly. Furthermore, utilizing professional skills in the sector of cyber audits incurs considerable additional expenditures.

References

1. Kearns GS. Cyber auditing: A systematic review. J Inf. Syst. Educ. 2016;27(2):117-136.
2. Pathak J. Information auditing and security. Hoboken: John Wiley & Sons; c2015.
3. Rittinghouse JW, Hancock WM. Cybersecurity operations handbook. Amsterdam: Elsevier; c2017.
4. Whitman ME, Mattord HJ. Principles of information security. 6th ed. Boston: Cengage Learning; c2018.
5. Hussein MK. Electronic government. J Baghdad Coll. Econ Sci. Special Issue of the College Conference; c2013.
6. Abu Shanab IA. E-Government as a tool for democracy and community development. Cairo: Arab Organization for Administrative Development; c2012.
7. Attia AA. The impact of the use of information technology on the job performance of workers in local government agencies. [Thesis]. Ouargla: University of Kasdi Merbah Ouargla. Faculty of Economic and Commercial Sciences; c2012.

Appendix

Questionnaire

Part 1: Demographic data

Gender	Male
	Female
Age	Less than 25
	25-35
	36-45
	More than 45
Qualification	High school and below
	Diploma
	Bachelor's
	Master's
	Ph.D

Part 2: Topics of the study

The first axis: Basic obstacles to cyber auditing

	Phrase	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	The complexity of an organization's technological infrastructure poses a challenge to cyber auditing.					
2.	The lack of qualified human resources in the field of cyber auditing hinders the effective implementation of operations.					
3.	Lack of clarity of roles and responsibilities between cyber audit teams and other departments affects efficiency.					
4.	The absence of senior management support to invest in cyber auditing limits an organization's ability to adapt.					
5.	Difficulty determining the scope and limits of cyber auditing due to the changing nature of risks.					

The second axis: Enhancing cyber auditing techniques

	Phrase	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Using advanced data analysis tools helps detect cyber threats faster.					
2.	Developing continuous monitoring programs for cyber activities enhances audit and response capabilities.					
3.	Adopting artificial intelligence techniques to analyse records and data improves the accuracy of audits.					
4.	Implementing data encryption mechanisms and regular backups increases the security of institutional data.					
5.	The use of standardized audit frameworks and protocols contributes to standardizing practices and improving effectiveness.					

The third axis: The role of advanced technologies in cyber auditing

	Phrase	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Advanced data analytics enables detection of anomalous behaviour patterns and potential threats.					
2.	Artificial intelligence applications help predict and respond better to cyber risks.					
3.	Automating audit and review processes using robots increases the efficiency and speed of audit procedures.					
4.	Using machine learning techniques to monitor and analyse data improves an audit's ability to detect breaches.					
5.	Integrating advanced cybersecurity technologies such as Blockchain enhances the integrity and security of data during audits.					

Fourth axis: Expenses and costs associated with a cyber-audit

	Phrase	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Investing the necessary resources in technology infrastructure is essential to effectively implement a cyber-audit.					
2.	Employing specialized competencies in the field of cyber auditing requires significant additional costs.					
3.	The need to train and develop the technical skills of the cyber audit team increases costs.					
4.	Acquiring advanced cyber auditing tools and systems requires significant financial investments.					
5.	Covering cybersecurity and risk insurance costs is vital but expensive.					

Fifth axis: Evaluate the impact of electronic auditing on data security and business continuity

	Phrase	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1.	Implementing cyber auditing on a regular basis improves the level of organizational data security.					
2.	Electronic audit procedures contribute to early detection of cyber threats.					
3.	Cyber audit results help develop continuity and disaster recovery plans.					

4.	Reports and analyses resulting from a cyber-audit increase management's awareness of risks.					
5.	Implementing cyber audit recommendations improves the ability to confront cyber-attacks.					