ISSN: 2633-4828 Vol. 6 No.1, January, 2024

International Journal of Applied Engineering & Technology

THE ROLE OF INTERNAL AUDIT COMMITMENT IN REDUCING CYBERSECURITY RISKS

Karar Jasim Najm[1] and Zahraa Musafer Obaid Al-Karaawi[2]
[1]Faculty of Administration and Economics, University of Kufa, Najaf, Iraq
E-mail: kararj.aleesawe@uokufa.edu.iq

[2]Faculty of Administration and Economics, University of Kufa, Najaf, Iraq
E-mail: zahraamusafer98@gmail.com

ABSTRACT
Companies operate in a dynamic environment constantly changing and exposed to various risks. One is cybersecurity. Through their multifaceted role, internal auditors can contribute to reducing information system breaches. However, the work available on the relationship between internal audit and cybersecurity worldwide is minimal and practically non-existent in the case of Greece. Thus, the purpose of this paper is to examine the variables that affect cybersecurity and which, at the same time, are Related to Internal Audits. In this context, methodologically, a questionnaire was distributed to companies in Iraq, and the researchers found an impact between internal audit and cybersecurity risk management.

Keywords: Internal Audit, Cybersecurity, audit risk management, internal control

I. INTRODUCTION
Cybersecurity encompasses the protocols and measures implemented to safeguard internet-connected devices, networks, and data, with the objective of thwarting unauthorized access and illicit exploitation. It encompasses techniques, resources, and concepts pertaining to information security and operational technology. The term "cybersecurity" is often employed interchangeably with information security or IT security. Nevertheless, it is imperative to recognize the substantial disparities among these regions. Cybersecurity encompasses the utilization of information technology for defensive and offensive objectives. The field is experiencing significant expansion as a result of the increasing menace of cybercrime and data breaches. Organizations across many industries such as finance, healthcare, and retail want professionals with expertise in cybersecurity. Nations and corporations worldwide are enacting strategies to prevent cybercriminal activities and safeguard the integrity of information. The cooperation between the public and private sectors is crucial in tackling cyber threats globally. Cybersecurity plays the role of protecting the integrity, confidentiality, and availability of information technology from attacks by unauthorized internal and external malicious forces and criminals. Business organizations have implemented a variety of procedures, policies, safeguards, and internal control measures. They are collectively referred to as cybersecurity risks and assessments (CSRAs) (Ajiji, 2019).

Companies are setting up cybersecurity to thwart attacks on their critical infrastructure, both public and private. These attacks include ransomware, malware, identity theft, and email phishing. The goal of cybersecurity is to prevent, mitigate, and monitor risks to protect critical infrastructures and maintain optimal productivity (Usman et al., 2021).

Although many studies have been conducted on cybersecurity, few have provided conceptual and theoretical insights into the role and characterization of internal auditors (Betti & Sarens, 2020a).

The success of the economic units depends mainly on the extent of harmony of the different departments in those economic units. Among those departments, we find risk management, as their performance depends on drawing up plans to respond to the expected risks and examining potential threats to the economic unit or its human resources and equipment to reduce them to a minimum. This paper seeks to fill this gap in existing studies by focusing on the role of internal features in assessing cybersecurity risks among business organizations based on Funding. The objectives of the paper are conceptualized if (1) the professional ethics of internal auditors enhance cybersecurity risk assessment in a financial business organization, (2) the internal auditor's personality trait affects

the cybersecurity risk assessment in a financial business organization, (3) the competence of the internal auditor's skills enhances the cybersecurity risk assessment to perform tasks in a finance-based business organization (4) the competence of internal auditors' knowledge of cybersecurity risk assessment affects the performance of the task in a finance-based business organization and (5) to determine whether internal auditors' deterrence and remuneration enhance cybersecurity risk assessment to perform tasks in financial organizations. The plausible reason for the global increase in cybercrime is individuals who lack cybersecurity awareness and weak management attitudes towards cybersecurity risks. And for the purpose of achieving the objectives of the research has been divided into four sections, section 2 included the presentation of literature, section 3 data and methodology, and section 4 results, conclusions, and discussion.

II. LITERATURE REVIEW

A. Internal Audit

Internal audit is a systematic and well-documented process that includes collecting audit data and evaluating the degree of compliance with auditing standards. This tool not only manages satisfactory standards, but also enhances the company's quality management system and significantly impacts the performance of testing and inspection laboratories as well as certification organizations. Internal audit facilitates management in identifying and analyzing risks, making informed decisions, and enhancing the risk control and management framework. It assists entities in both the public and private sectors by evaluating the entity's control and risk management procedures and business concepts. Internal audit contributes to business risk management by examining and evaluating risk management procedures, thus facilitating the development of simpler processes. An audit is a self-sufficient, unbiased endeavor that enhances an organization's operations by evaluating and enhancing risk management, control and governance procedures. Internal audit has gone through some developments during the years, including before 1940; it was an assessment of the credibility and accuracy of the high office and clear evidence of misrepresentation and errors (Hussein, 2020). In addition, internal audit will not be far from the rapid developments that the world has witnessed recently, especially the information revolution that affects all life activities, which is expected to keep pace with these developments by following new techniques and specialized and logical strategies at a high level so that the audit is in its practical form instead of the familiar methods used recently, as these strategies are granted to internal audit departments and units to change their strategies in the field of examination and increase the additional value of economic units. (Mohammedi,2020)

It is challenging to set limits for the types of internal audit due to the breadth of the scope of audit for all tasks in the economic unit, and its task is to evaluate the adequacy and effectiveness of the cycles and operational processes of the economic unit's work, as this shows the extent of internal audit applications and wide because it depends on the internal control of the unit and the evaluation and the degree of observance of regulations and guidelines for that they are separated (Benyounes & Boudelmi, 2021). The quality of the audit assumes a vital role in protecting economic units from the risk of collapse, and this is the goal that all economic units are looking for, meaning that units whose operations are checked by professional auditors face less risk (HAZAEA et.al.,2020). The independence of the internal audit department was recognized as one of the critical parts of successfully mastering the internal audit function, and standard-setters, as well as professional bodies, gave greater importance to the possibility of internal audit independence even though they are employees within the economic unit (Musah, 2018).

Risk is often used in an ambiguous way, so a precise definition has been sought that includes all components of risk, such as uncertainty, measurement of uncertainty, loss, and financial estimation of loss; risk is defined as the probability of an uncertain event leading to economic loss (Thoyts, 2010). The godfather of management, Henri Fayol, believes that safe management is the cornerstone of effective management, and for safe management to be protected, there must essentially be a skilled authority whose primary task is to promote well-defined courses of action to anticipate risks around economic unity and try to stay away from it (Nasira,2023). As a result, the strategies and equipment the economic unit has chosen to use to manage such risks must be identified (Bachy & Harache, 2010).

B. Cybersecurity Risk Management

Cybersecurity risk management entails assessing and reducing risks associated with cybersecurity threats in order to ensure the security and efficiency of information systems and process control systems. It is essential to understand potential threats, vulnerabilities and mission consequences, as well as make informed judgments to balance security and functionality. It is necessary to adopt a proactive strategy to create preventive and flexible mechanisms during the acquisition and development process. In addition, incorporating qualitative and semi-quantitative analyzes may enhance the decision-making process. Cybersecurity risk management technology must be applied repeatedly throughout the life of the system, in accordance with national cybersecurity policies and standards. The process of managing cyber risks in medical devices involves identifying and evaluating potential risks, determining whether they are acceptable, adopting strategies to mitigate the risks, and providing a rationale for the trade-off between risks and benefits. Effective cyber risk management is critical for organizations, necessitating proper oversight, assessing vulnerabilities, and prioritizing problem resolution. The most essential elements of cybersecurity are the technologies used to protect the information and data of the economic unit from any unauthorized access, manipulation, or use to maintain its confidentiality, grant access to it at any possible time, and maintain its reliability from any unexpected attack which has a significant impact on the performance of the unit, and its ability to change course quickly in response to events and its environment, as well as its continuity and survival for the most extended period (Mahdavifar & Ghorbani, 2019).

The methods and procedures used in cybersecurity to protect computers and networks, reduce hacking attempts, maintain databases and address other risks, and enable the advancement of information technology and the Internet while minimizing the risks that may harm them (Wu et al., 2018). Protecting systems, networks, and programs from cyberattacks that typically seek to access, modify, or destroy sensitive information, solicit user funds, or disrupt business operations (Mohammed, 2021). Protecting the Unit's assets and resources from organizational, human, financial, technical, and information threats will enable it to accomplish its mission. (Crossed out Wolkhwaider, 2018Cybersecurity is critical to work across the board, but it is essential to work with economic units (Al-Mutairi, 2022). Cybersecurity threats to individual and enterprise systems can target applications of cloud computing systems, financial transactions, infrastructure, information, data, and networks (Bouveret, 2018). Internal audit and cybersecurity are new dimensions of security practices aimed at supporting the protection of critical information assets of units. The audit will seek evidence of organizational information security policies and their effectiveness in protecting asset integrity, data confidentiality, and data access and availability. Essentially, the audit assesses a unit's effectiveness in protecting its valuable or critical assets. Information systems security management is increasingly vital to units as units rely on technology to conduct business, create competitive advantage, and achieve higher returns on investment (Islam et al., 2018). Economic units have worked hard in recent years to find more efficient ways to improve their performance while maintaining market share and gaining a competitive advantage. A robust internal control system, one of the components of which is the internal audit process, which aims to add value and improve procedures, plays a vital role in preventing cyber-attacks and encouraging managers to reduce risk (Lois et.al., 2020).

III. DATA AND METHODOLOGY

A questionnaire form was designed according to the Likert five-point scale, and for the purpose of testing research hypotheses, 100 questionnaire forms were distributed, and 85 questionnaire forms were retrieved, and to test research hypotheses statistically, SPSS V.23 was used.

IV. RESULTS

Testing the hypothesis that states, "**There is a statistically significant impact of internal audit on cybersecurity risk management.**"

To test this hypothesis, the linear regression" model was formulated:

$CS = B0 + B1\ IA + E$

Where: -

IA = Independent Variable (Internal Audit).

CS = intermediate variable [1](cybersecurity risk).

E = estimation errors or so-called statistical remainders.

B0 = The constant of the regression equation which represents the dependent variable's value when the independent variable's value is equal to zero.

B1 = slope of the regression function, which measures the effect of the independent variable on the dependent variable.

Table 1. The summary of the first sub-hypothesis test model.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.868a	0.754	0.751	0.169
a. Predictors: (Constant), IA				
b. Dependent Variable: CS				

Source: Prepared by the researchers based on the SPSS v.23 program

The model summary table above shows that the correlation value (R between the variables) was 0.868, a high strength value and that the R Square determination coefficient was 0.754, representing" The independent variable (internal audit) explains 75.4% of the intermediate variable (cybersecurity risk), and the standard deviation of the Std. The error of the Estimate was .1690, which is a deficient number. The lower this type of error, the better it is statistically.

Table 2. Hypothesis Test Variance

Model		Sum of Squares	Df 2	Mean Square	F	Say.
1	Regression	7.289	1 3	7.289	254.250	0.000b
	Residual	2.380	83 4	0.029		
	Total	9.669	84 5			
a. Dependent Variable: CS						
b. Predictors: (Constant), IA						

Source: Prepared by the researchers based on the SPSS v.23 program

[1] It should be noted that the intermediate variable is treated as a dependent variable by measuring the effect of the independent variable in it and is treated as an independent variable when measuring its effect on the dependent variable.

df2 stands for degrees of freedom and represents the number of values that can be changed in the calculation of a statistical property. The calculation of various statistical properties is based on a set of information or data. It is called the number of information independent of each other that goes into the calculation of a particular statistical property.

Refers3 to the first degree of freedom, which is equal to the number of independent variables in the regression model used to measure the hypothesis.

refers4 to the second degree of freedom and is equal to the sum of the two degrees of freedom minus the first degree of freedom.

Refers5 to the sum of the first and second degrees of freedom and is equal to the sample size minus one.

The table above shows the variance above ANOVA that the calculated value of F was 254.250, which is greater than its tabular value calculated according to the degrees of freedom of (83.1) of 3.96 at a significance level of 5%. The significance level of the Sig test was 0.000 is less than the predetermined error value in the social sciences by 0.05, which indicates the appropriateness of the statistical model used to test the hypothesis.

Table 3. Coefficients of the regression function of the hypothesis

Model		Unstandardized Coefficients		Standardized Coefficients	T	Say.
		B	Std. Error	Beta		
1	(Constant)	0.602	0.235		2.567	0.012
	Audit Hub	0.866	0.054	0.868	15.945	0.000
a. Dependent Variable: CS						

Source: Prepared by the researchers based on the SPSS v.23 program

The Coefficients table shows that the value of the regression **equation constant** was 0.602, and the slope of the regression B_0 equation was 0.866, B_1 which shows the effect of the independent variable on the whip variable (by the coefficient B), and the positive value of the coefficient indicates that there is a direct effect between the independent and median variables, in other words, any increase in the independent variable (internal audit) B_1 By one degree leads to an increase of 86.6% in the intermediate variable (cybersecurity risks) with the stability of all other independent variables, and it is noted from the above table also that the level of significance of the T-statistic for the independent variable reached 0.00, which is much less than the accepted error in the social sciences and predetermined by 0.05, and this means that the sample data have provided convincing evidence of the rejection of the nihilistic hypothesis and the acceptance of the alternative hypothesis The effect is statistically proven and therefore there is a statistically significant positive (positive) impact of internal audit on cybersecurity risks. The following figure confirms the direct relationship between the two variables through the upward trend of the curve:

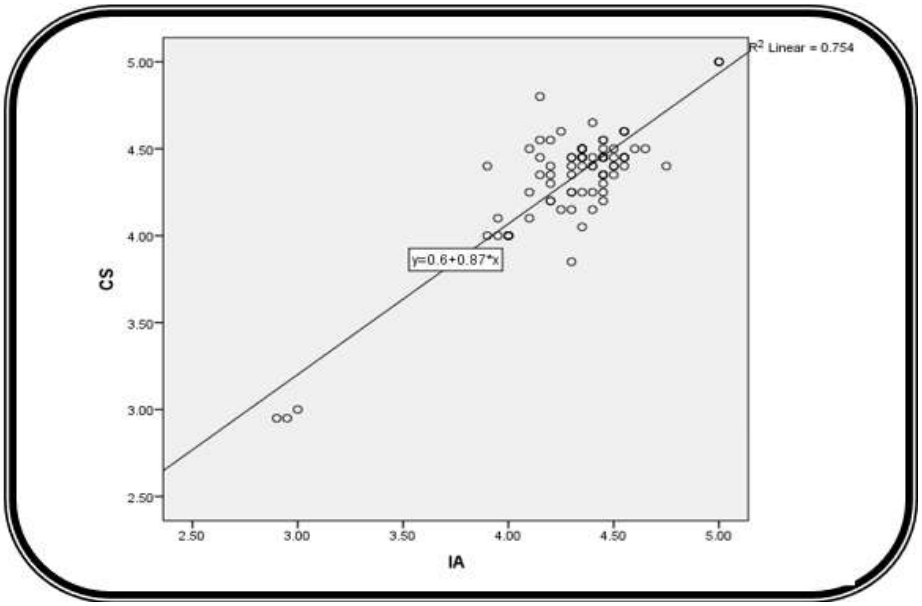

Figure 1. Relationship between Internal Audit and Cybersecurity Risks

The regression equation adopted in the hypothesis test can be reformulated in the light of the results reached, which can be used for prediction as follows:

CS = 0.6 + 0.8* IA

The following figure presents the histogram showing the normal distribution of the regression equation's statistical remainders and the accuracy of the previous regression equation.

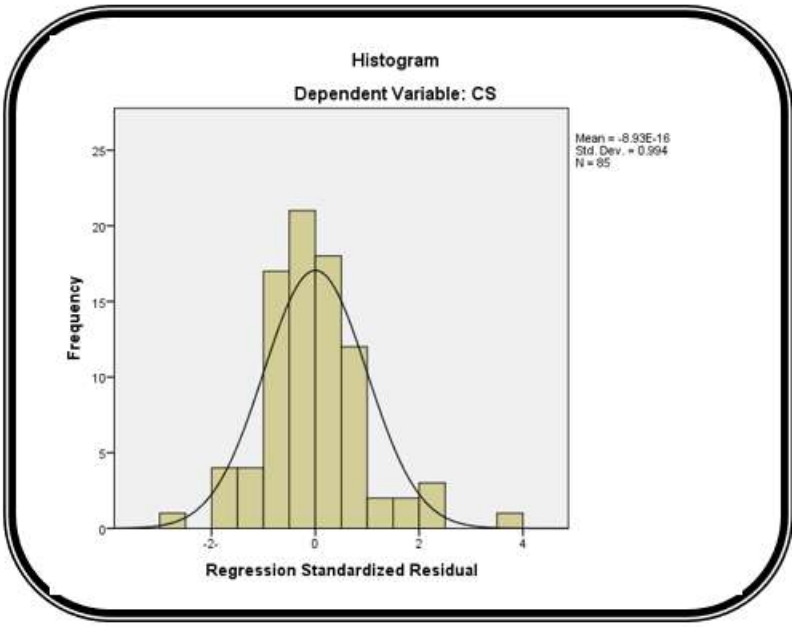

Figure 2. A histogram of hypothesis residuals

The following figure graphically shows the fulfillment of the conditions of the regression analysis test, which shows the distribution of points around the straight line, and this proves that the statistical remainders follow the normal distribution**.**

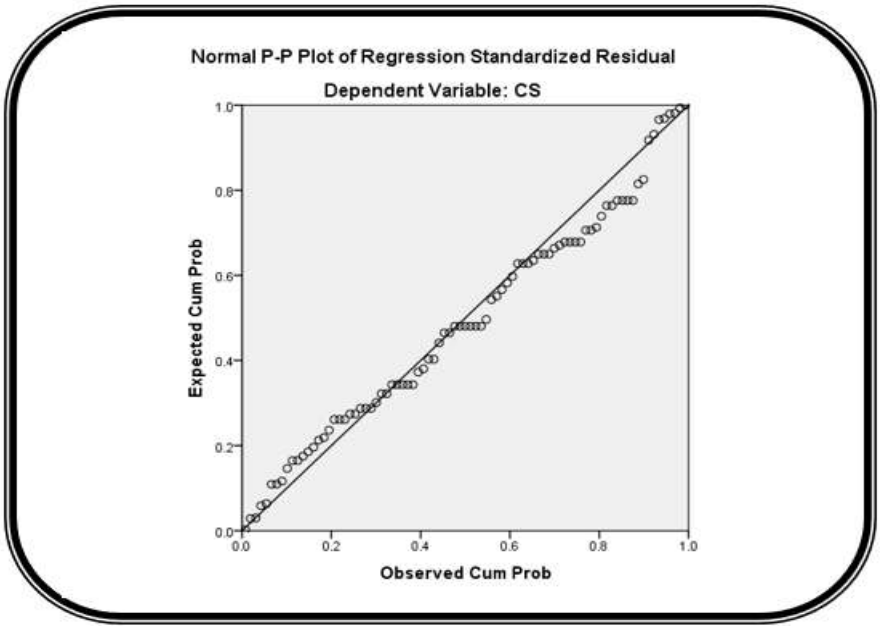

Figure 3. Normal distribution of the hypothesis remainders

V. CONCLUSIONS AND DISCUSSION

Cybersecurity risk management is a critical concern for organizations, especially in the banking sector. Internal audit teams are essential for guaranteeing the robustness and efficiency of cybersecurity governance measures in banks. Audit committees were required to confront emerging security concerns and comprehend the culprits behind cybercrimes in order to consider the risks associated with cybersecurity. External auditors are responsible for auditing cybersecurity risks and assessing their impact on organizational continuity. The efficacy of internal audit in cybersecurity is assessed using the Cybersecurity Audit Index, which encompasses the aspects of planning, performance, and reporting. Index scores exhibit variability, demonstrating a positive association between the effectiveness of cybersecurity audits and the maturity of cyber risk management. Nevertheless, the signal is unrelated to the potential occurrence of a cyber assault. Internal audit teams and external auditors have crucial responsibilities in overseeing and evaluating cybersecurity threats within firms. Robust departmental security and online data standards are essential for all enterprises as the transition to digital platforms becomes increasingly prevalent. The internal audit has undergone changes and enhancements in its duties, and it should also contribute to enhancing the security of online services through various means. The consequences of the extensive investigation initiative delineate the pressing imperative of doing internal audits to ensure the security of data frameworks. The conclusions derived from meticulous investigation are highly conclusive. Initially, many companies are referred to as corporations. The perpetuation of abusive practices within these companies is a tangible reality that tends to escalate with time. Ensuring the readiness of auditors is crucial, given the strong correlation between security and the regulations provided by each organization. Furthermore, auditors must broaden their perspective on digital security matters in order to align their endeavors with experts in the industry. The auditors' consultative role remains unchanged. Their collaboration with the Board in establishing the arrangements is vital for implementing network security measures. Nevertheless, it is evident that auditors who possess expertise in circumventing network security threats may demonstrate reduced proficiency when confronted with actual automated attack scenarios. Auditing continues to be a strong area of the organization, known for its proven effectiveness and quality. The requirements for the functional audit throughout the digitization phase will depend on the auditors' capacity to incorporate digital wellness into their training program. Furthermore, during the implementation of internal audit and cybersecurity risk management in the Iraqi context, it was seen that there is a correlation between internal audit and cybersecurity risk management. The internal audit function is essential for examining cybersecurity risks and assuring the uninterrupted operation of the organization. Audit committees were required to confront emerging security concerns and comprehend the culprits behind cybercrimes, all while guaranteeing that staff had adequate training to assess cybersecurity hazards. An analysis was conducted on the role of external auditors in assessing cybersecurity risks. The findings revealed that organizations are increasingly using electronic accounting systems, but audit teams lack the necessary expertise to effectively audit cybersecurity risks. Furthermore, external auditors exhibit greater scrutiny towards organizations that have experienced a cybersecurity breach by imposing elevated audit costs. This signifies their recognition of heightened risks and their increased diligence in auditing such companies. Internal and external auditors have a crucial role in evaluating and overseeing cybersecurity threats within firms.

REFERENCES

Ajiji, Y. M. (2019). Cybersecurity Issued in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available, 7(April 2017). https://doi.org/10.23956/ijarcsse/V6I12/01204

Al-Mohammedi, Y. A. (2020, November). The Role of Digitalization in Developing Internal Audit Practices in an IT Environment. In 2020 2nd Annual International Conference on Information and Sciences (AiCIS) (pp. 230-236). IEEE.

Mutairi, Khalid Zahir Abdullah. (2022). "The Role of Penal Legislation in Protecting Cybersecurity in the -Al .1066-GCC Countries". Journal of Jurisprudence and Legal Research, 28: 969

Bachy, B. (2010). Harache C. (coordinated by). All the functions. Management. Paris: Dunod.

Ben Younes, Elham and Boudelmi. (2021). "The Role of Internal Audit in Inventory Control". Master's Thesis, Mohamed Boudiaf University, Faculty of Economic, Commercial and Management Sciences.

Betti, N., & Sarens, G. (2020a). Understanding the internal audit function in a digitalised business environment. Journal of Accounting & Organizational Change © EmeraldPublishingLimited 1832-5912 https://doi.org/10.1108/JAOC-11-2019-0114

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.

Crossed out, Rima and Lakhwaider. (2018). "The Role of Cybersecurity in Addressing Commercial Terrorism."

Hazaea, S. A., Tabash, M. I., Khatib, S. F., Zhu, J., & Al-Kuhali, A. A. (2020). The impact of internal audit quality on financial performance of Yemeni commercial banks: an empirical investigation. The Journal of Asian Finance, Economics and Business, 7(11), 867-875.

Hussein, Faten Ali. (2020). "The Impact of Project Resource Planning (ERP) System on the Quality of Internal Audit in accordance with the International Standards for the Professional Practice of Internal Auditing". Master Thesis, University of Kufa, College of Administration and Economics.

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, 33(4), 377-409.

Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business, 15(2), 205-217.

Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. Neurocomputing, 347, 149-176.

Muhammad, Amna Ali Bashir Muhammad. (2021). "Cybersecurity in the Light of the Purposes of Sharia". Journal of the Faculty of Islamic and Arabic Studies for Girls in Alexandria, 37(1): 449-505.

Musah, A. (2018). Determinants of internal audit effectiveness in State-Owned Enterprises (SOEs) in Ghana. In Determinants of internal audit effectiveness in state-owned enterprises (SOEs) in Ghana: Musah, Alhassan.

Thoyts, R. (2010). Insurance theory and practice. Routledge.

Usman Alih, Elaigwu M. &Salau R.K. (2021). Cybersecurity Risk Assessment and The Role of Internal Audit Function Among the Listed Financial Companies in Nigeria: A Global Empirical Perspective.Creative Journal of Business Research. Vol.1. No.1 2021

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. Journal of manufacturing systems, 48, 3-12.