The Effectiveness of Internal Auditing in Mitigating Cybersecurity Risks

-A Field Study –

Dr.Basheer wakas

PhD in Accounting -Accounting Department- Faculty of Economics-Damascus University

Abstract:

This research paper examines the effectiveness of internal audit in mitigating cybersecurity risks in Syrian banks. To achieve the study's objectives, a descriptive and analytical approach was used to analyze the direct impact of internal audit efficiency and effectiveness on cybersecurity standards. To test the research hypotheses, a linear equation analysis was conducted using SPSS to conduct statistical analysis and validate the results. In addition, a questionnaire was distributed to collect relevant data and provide additional insights for the study. A structured questionnaire was developed with a five-point Likert scale. Of the 100 questionnaires distributed, 86 were completed and returned for analysis. The research identified several key findings, the most important of which was the positive impact the efficiency and effectiveness of internal audits have a high effect of(0.75)significant at (sig .000) on the mitigating cybersecurity risks of Syrian commercial banks. Recommend study to Enhance training and professional development, develop information security governance policies, Implement data analytics techniques.

Keywords: Internal audit, Cybersecurity, Effectiveness, Information security risks.

General framework of the study

1-Introduction:

The digital age has revolutionized many industries, including accounting, thanks to the widespread use of technology. The emergence of digital accounting systems, cloud computing, and online financial transactions has increased the accounting sector's reliance on digital tools and platforms. This has made accounting systems vulnerable to cybersecurity threats. Cybersecurity, the practice of protecting systems, networks, and software from digital attacks, has emerged as a major concern for accounting professionals. The increasing frequency of cyberattacks has placed organizations under immense pressure as they struggle to combat the growing sophistication, prevalence, and complexity of cybercrimes. These attacks have impacted both the financial and non-financial sectors, resulting in increased costs and financial losses, reduced market share, and diminished stakeholder confidence (World Economic Forum, 2023; Osuagwu, 2022). Meanwhile, traditional audit procedures, which aim to verify the adequacy and effectiveness of anti-fraud mechanisms, have consistently failed to detect and prevent cyber threats (Beredugo, Inah, & Edom, 2014). Therefore, it is essential that auditors across all sectors integrate cybersecurity into their audit plans, continually assess the effectiveness of cybersecurity tools, and report all cybersecurity exposures to the board of directors for appropriate action (CBN, 2022).[1]

2-Problem of the study:

Many organizations are constantly exposed to cybersecurity risks, making managing them without disrupting essential services difficult. Most studies indicate that cybersecurity risks have increased significantly in most organizations recently and are constantly evolving rapidly and unpredictably.

Cybersecurity relates to the processes and practices designed to protect an organization's information assets and technologies from cyber threats and attacks by implementing corrective actions (Neal and Draven, 2019). Therefore, many organizations will not survive any cybersecurity attacks without protecting their most valuable information assets, and therefore, this must remain a critical aspect that all organizations must address daily[2] .

With the increasing number of cybersecurity breaches, internal audit can play an effective role in managing and mitigating cybersecurity risks and ensuring the effectiveness of controls through planning and evaluating cybersecurity processes and tools. This practice is relatively new in most organizations in Syria, and there is a lack of research on the effectiveness of cybersecurity

[1] Beredugo S. B(2024), "Cyber security Audits And The Mitigation Of CyberAttacks Of Selected Companies In Nigeria", International Journal of EGovernment & E-Business Research, Vol. 9, Issue 1, 2024, pp 19-35, DOI: https://doi.org/10.53882/IJEGEBR.202 4.0901003.

[2] Dikokoe.t(2021):" Role of Internal Audit in Managing Cyber Security Risks". Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII in COMPUTER AUDITING In the COLLEGE OF BUSINESS AND ECONOMICS at the UNIVERSITY OF JOHANNESBURG.

audits in preventing cyberattacks in Syria. Therefore, it is necessary to evaluate the role of internal audit in this regard, which this study seeks to achieve. In light of these challenges. [3]. The problem of this study is reflected through the following questions:

Main Research Question: To what extent is internal audit effective in reducing cybersecurity risks?

The following are the sub-questions derived from the main question:

--To what extent is internal audit effective in reducing cybersecurity risks through the application of security policies and procedures and the effectiveness of security controls?

-To what extent is internal audit effective in reducing cybersecurity risks through the detection of and response to cybersecurity incidents?

-To what extent is internal audit effective in reducing cybersecurity risks through compliance with legislative requirements and employee training?

3-model of Study:

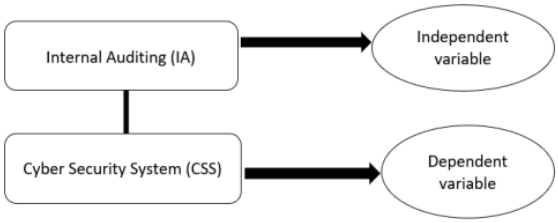

Figure 1. Research model

-Independent Variable: Effectiveness of Internal Audit. This can be measured through several sub-dimensions:

-Dependent Variable: Reduction of Cybersecurity Risks. This can be measured through several indicators:

a) Level of application of information security policies and procedures.
b) Efficiency of implemented security controls (technical, administrative, physical).
c) Ability to detect and respond to cyber incidents.
d) Level of employee awareness of cybersecurity risks.
e) Extent of compliance with legislative and regulatory requirements related to cybersecurity.

4-Previous studies:

-Babiker I. (2025): Purpose: This study investigates the role of internal audit procedures in enhancing cybersecurity effectiveness. It seeks to answer key questions: Is the efficiency and effectiveness of internal audits indicative of proper cybersecurity standards? To what extent can audit committees improve internal audit efficiency and achieve information security? How do information security governance standards help mitigate cybersecurity risks? To address these questions, the opinions of 30 internal auditors from Saudi Arabia, Sudan, and Egypt were surveyed. A descriptive and analytical approach was used. The findings reveal a positive relationship between the efficiency and effectiveness of internal audits and enhanced cybersecurity. Specifically, a more effective internal audit system correlates with stronger information security, and improvements in information security governance standards significantly reduce electronic risks. This study emphasizes the crucial role of internal auditing in strengthening cybersecurity from the auditors' perspective, focusing on its impact on auditing frameworks and security strategies. As one of the few studies addressing this intersection, it provides valuable insights and recommendations for stakeholders in both fields.

-Rofi'ah, D. M. (2025): This study interprets the application of the NIST Cybersecurity Framework (CSF) by Indonesian internal auditors. Employing Paul Ricoeur's hermeneutic phenomenology and Interpretative Phenomenological Analysis (IPA), this research delves into the meaning of CSF from the perspective of internal auditors, including its adaptation to local organizational culture and the factors shaping its effectiveness. Key findings reveal that CSF transcends its role as a technical guide, acting instead as a driver for cybersecurity culture transformation. This study's implications emphasize the necessity of cross-departmental collaboration, context-specific security policy departments, and the enhancement of internal auditor competencies. The novelty of this research lies in its application of in-depth interpretative analysis, showing CSF as an adaptive tool fostering cybersecurity systems attuned to Indonesia's unique characteristics.

[3] Abu Nassar. M, Hamidat. J, (2016), International Accounting and Financial Reporting Standards, 3rd ed, Amman, Wael Publishing House, 52

- (Alhawtmeh. O. M,2025): This paper investigates the role of internal audits as an instrument for enhancing the effectiveness of cyber security in Jordanian government agencies. To accomplish the study's objectives, a descriptive and analytical approach was used in analyzing whether the efficiency and effectiveness of IA directly influence cybersecurity standards. To investigate the research hypotheses, an analysis was conducted using linear equations utilizing SPSS software to perform statistical analysis and validate the findings. Additionally, a questionnaire was distributed to gather relevant data and provide further insights for the study. A structured questionnaire incorporating a five-point Likert scale was developed. Of the 100 questionnaires distributed, 84 were completed and returned for analysis. The research identified several key findings, with the greatest being the statistically significant influence of internal auditing on enhancing CS effectiveness and its subsequent effect on insurance costs.

-Beredugo S. B(2024),: Aim of the Study: The study is dedicated to addressing two critical questions: Can cyber security audits effectively reduce cybercrimes in Nigeria? And, is the use of cyber security tools to mitigate cyberattacks by the financial sector significantly different from that of the non-financial sectors in Nigeria? . The survey design was used to collect information from 125 respondents, cutting across the regional headquarters of 32 selected companies in the South-West and the North-West regions in Nigeria as a means to explore the aim of the study through ordinary least square and independent t-tests analysis. Findings: The results show that cyber security audit can assist in averting cybercrime. The result also indicated that there is no significant difference in the cyber security tools used, between the financial and non-financial sectors in mitigating cyber-attacks in Nigeria. The study demonstrates that integrating cyber security audits into companies' practices can significantly reduce vulnerability to cyber-attacks. By incorporating cyber security tools into audit plans and regularly evaluating their operational effectiveness, Nigerian firms can fortify their defenses against potential threats. The study delved into whether the use of cyber security tools in curbing cyber-attacks in the financial sector differs significantly from that in the non-financial sectors in Nigeria. The research conclusively demonstrated that organizations armed with robust cyber security audit architecture can effectively repel all cyber threats and attacks.

-Gogineni , S(2023): This paper's goal is to examine how well cybersecurity internal audits work. For this reason, set out to create a Cybersecurity Audit Index that covers the bases in terms of preparation, execution, and reporting. postulate that the likelihood of a successful cyber assault is inversely related to the efficacy of cybersecurity audits and that cyber risk management maturity is favorably related to them. By surveying auditors and chief audit executives from different nations and industries, the study able to test our hypotheses. research shows that there is a wide range of Cybersecurity Audit Index scores (58 on a scale from 0 to 100). Cyber risk management effectiveness reporting to the Board of Directors is less strongly tied to the planning and performance stages, despite the high and positive correlation between them. Although it was expected that the Cybersecurity Audit Index would have a positive correlation with maturity, it was surprised to see no correlation with the likelihood of a successful cyber assault. For the first time, this report quantifies the impact of cybersecurity audits on cyber risk management and how effective they are.

-Usman, A., Che-Ahmad, A., Abdulmalik, S. O. (2023): This paper aims to establish a theoretical framework that will enhance the examination of the role of internal auditors in cybersecurity risk assessment in financial based business organizations. Financial-based business organizations are institutions or companies that render financial services to public and private stakeholders in an economy. It is a powerful sector in the economy of every country. This drive poses a lot of challenges to organizations. Hence, business organizations strategically devised a means to safeguard the integrity, confidentiality, and availability of information. Also, innovation poses many risks and threats to the internal audit function in an organization. Using the competency and planned behavior theories (McClelland 1973 and Ajzen,1991), this study disclosed that the task performance of cybersecurity risk assessment by the internal auditor is influenced by the required internal auditor's characteristics of professional ethics of integrity and objectivity, personality traits, professional skills competency professional knowledge competency and deterrence and rewards to advise the management on the implications of cyber security risk on business organizations for monitoring and mitigations. A literature review approach is adopted to highlight the role of internal auditors in cyber security risk assessment in financial–based business organizations.

- Usman, A., Elaigwu, M., & Rofeekat, K. (2021).: This study is aimed at exploring the empirical review of the role of internal audit function on the mitigation of cyber security risks among the listed financial companies in Nigeria from the conceptual perspective. This research examined three factors that would most likely affect the conceptual outcome of internal audit functions in managing cyber security in Nigeria financial Institutions. Those factors are IAF internal policy, IAF risk control, and IAF technical awareness ON the mitigation of cyber security risks among the listed financial organizational. This study employed secondary data with content analysis of extant studies across the globe to conceptually examine the impact and applicability of IAF in the Nigeria financial companies. A total of 100 extant studies were reviewed from reputable articles on the sample firms. Findings from this study indicates concrete prepositions that all the three identified factors have positive and significant relationship with the effectiveness of internal audit function in managing cyber security risk in Nigeria Financial Companies.

-Vuko. T, Čular. M, Drašček . M, SLAPNIČAR. S (2021):We analyze which factors explain the effectiveness of internal audit in providing assurance about cybersecurity risk management. Based on neo-institutional theory, we hypothesize that coercive (cybersecurity regulation), normative (internal auditors' academic background, cybersecurity certifications, and training) and mimetic forces (outsourcing) positively contribute to cybersecurity audit (CSA) effectiveness. We extend the model of isomorphic

forces by the Board's support, Board's competencies, and the level of internal auditors' cooperation with the first and the second line of defense. To test our hypothesis, we conducted a survey involving 183 IT auditors and Chief Audit Executives from various industries, organizations of different sizes, and countries. We examined the relationships between CSA effectiveness and the hypothesized factors in a series of regression analyses and with a machine learning method – LASSO. We find that normative forces (cybersecurity certifications of the internal auditors) and human agency factors significantly explain CSA effectiveness.

Commenting on previous studies:

Key Themes and Focus Areas in the Reviewed Studies:

Role and Effectiveness of Internal Audit in Cybersecurity: The majority of the studies investigate how internal audit functions contribute to enhancing cybersecurity effectiveness, assessing risks, and ensuring compliance (e.g., Babiker, 2025; Alhawtmeh, 2025; Beredugo, 2024; Gogineni, 2023; Usman et al., 2023 & 2021; Vuko et al., 2021).

Frameworks and Methodologies: Studies explore the application of specific frameworks like the NIST Cybersecurity Framework (Rofi'ah, 2025) or aim to develop new ones like a Cybersecurity Audit Index (Gogineni, 2023). Methodologies are diverse, ranging from surveys and quantitative analyses to phenomenological and literature-based approaches.

Influencing Factors: Researchers examine various factors influencing cybersecurity audit effectiveness, including the efficiency of internal audits, audit committee roles, governance standards, auditor competencies (ethics, skills, knowledge), organizational culture, and institutional forces (coercive, normative, mimetic).

Geographical and Sectoral Context: Many studies are rooted in specific geographical contexts (Middle East, Indonesia, Jordan, Nigeria), highlighting regional perspectives and challenges. Some also focus on particular sectors like financial institutions or government agencies.

Outcomes: The studies generally find a positive relationship between effective internal auditing practices and improved cybersecurity posture, risk mitigation, and even impacts on aspects like insurance costs.

Previous studies have had diverse objectives and varied approaches to addressing the topic of cybersecurity and internal auditing. The current study will examine the effectiveness of internal auditing in mitigating cybersecurity risks in Syrian banks. To the best of our knowledge, the researcher has not found any studies related to our topic in Syria.

5- Research Objectives:

Main Objective: To evaluate the effectiveness of internal audit in reducing cybersecurity risks in Syrian banks.

Sub-objectives:

-Identifying the main internal audit practices and procedures related to assessing and managing cybersecurity risks.

-Measuring the level of application of these practices from the perspective of internal auditors and information security officers.

-Analyzing the relationship between internal audit characteristics s and its effectiveness in reducing cybersecurity risks.

-Providing recommendations to enhance the role of internal audit in addressing cybersecurity threats.

6-Importance of the study:

The importance of the research stems from the importance of the variables it includes, which can be summarized as follows:

A. This session addresses a critical topic: how to protect human and financial resources associated with information technology from cybersecurity risks, and how to manage these risks through the three lines of defense (information technology, cybersecurity, and internal audit functions). Cybersecurity is considered one of the most pressing risk management challenges for organizations across various sectors. Accordingly, the researcher emphasizes the importance of studying the reality of cybersecurity in Syrian banks, given its importance and direct impact on the national economy and society.

B. Explain the role of international professional organizations in the era of electronic globalization in addressing the risks that internal auditing may pose to the cyber environment of economic units, and in providing adequate protection for information, networks, and programs to achieve cybersecurity.

C. Provide internal auditors with an appropriate mechanism that enables them to respond to cyberattacks and expand the scope of cybersecurity knowledge to achieve digital auditing efficiency.

7 -Research Hypotheses:

Based on the theoretical frameworks and previous empirical findings, the following hypotheses were proposed:

Main Hypothesis: There is a statistically significant positive correlation between the effectiveness of internal audit and the level of reduction of cybersecurity.

Sub-hypotheses:

ph1-There is a statistically significant relationship at the significance level ($\alpha < 0.05$) indicating the effectiveness of internal audit in mitigating cybersecurity risks through the application of security policies and procedures and the effectiveness of security control

ph2-There is a statistically significant relationship at the significance level ($\alpha < 0.05$) indicating the effectiveness of internal audit in mitigating cybersecurity risks through the detection of and response to cybersecurity incidents

ph3-There is a statistically significant relationship at the significance level ($\alpha < 0.05$) indicating the effectiveness of internal audit in mitigating cybersecurity risks through compliance with legislative requirements and employee training

8 -Methodology of the Study:

The descriptive-analytical approach was followed in conducting the study, based on the nature of the subject, the studies, scientific references, and information obtained, and because it is one of the most widely used methodologies in studying social and human phenomena .Primary and secondary sources were used in the study. Primary data were collected through the distribution of a questionnaire, while secondary sources consisted of books, specialized scientific journals, research papers, and academic theses/dissertations. The questionnaire data were then inputted (or coded) and analyzed using the SPSS data analysis program, and appropriate statistical methods were employed.

9 -Study population and sample:

The target audience (internal auditors, information security managers, information technology managers in Syrian banks. As for the sample, the researcher was able to obtain a random sample comprising" 86 analyzable questionnaires".

10-Limits of the study:

-Spatial limits: The Syrian Arab Republic

- Time limits: The study was conducted in the year 2025.

Results and Recommendations

The researcher results the following:

-The positive impact the efficiency and effectiveness of internal audits have a high effect of(0.75)significant at (sig .000) on the mitigating cybersecurity risks of Syrian commercial banks.

-The positive impact the efficiency and effectiveness of internal audits have a high effect of(0.73)significant at (sig .000) on the mitigating cybersecurity risks through the application of security policies and procedures and the effectiveness of security controls of Syrian commercial banks.

- The positive impact the efficiency and effectiveness of internal audits have a high effect of(0.69)significant at (sig .000) on the mitigating cybersecurity risks through the detection of and response to cybersecurity incidents of Syrian commercial banks.

- The positive impact the efficiency and effectiveness of internal audits have a high effect of(0.72)significant at (sig .000) on the mitigating cybersecurity risks through compliance with legislative requirements and employee training of Syrian commercial banks.

The study results revealed that banks place great importance on having an internal audit function to assist management in assessing the effectiveness and adequacy of controls to mitigate cybersecurity risks. The results also highlighted a high level of compliance with internal audit standards. The results also demonstrated that some banks have highlighted their cybersecurity risks, with some conducting risk assessments to identify cyber threats and security breaches to improve cybersecurity risk management processes. The study results revealed that the internal audit function identifies and contributes to cybersecurity within banks by integrating cybersecurity reviews into the internal audit plan and assessing the adequacy of internal controls designed to mitigate cybersecurity risks.

The study recommended:

1.Enhance training and professional development: Provide ongoing training for internal auditors on the latest cybersecurity technologies and best practices.

2. Develop information security governance policies: Regularly review and update governance policies to align with global standards, including clear performance metrics and risk assessment procedures.

3. Implement data analytics techniques: Use advanced data analytics to monitor unusual activity and proactively identify potential risks.

4. Enhance cross-team communication: Improve collaboration between internal audit teams, cybersecurity departments, and senior management to enhance security strategies and resource allocation.

Références

1. Abu Shaaban, R (2016): "The Role of Internal Auditing in Assessing Operational Risk Management: An applied study on banks operating in the Gaza Strip" - p. 22.
2. AL Brazngi. S, Al-Saqa.z(2023):" Internal Audit Requirements to Enhance Cybersecurity in Economic Units in considering the Institute of Internal Auditors (IIA) Guidelines "Tikrit Journal of Administrative and Economic Sciences, Vol. 19, No. 63, Part (2): 94-112 Doi: www.doi.org/10.25130/tjaes.19.63.2.5.
3. Alhawtmeh. O. M,2025 "The role of internal audit as a tool for enhancing cybersecurity effectiveness in Jordanian government agencies", Heritage and Sustainable Development, HSD Vol. 7, No. 1, 2025, pp.319- 330.
4. Ardianto, A., Anridho, N., Ngelo, A. A., Ekasari, W. F., & Haider, I. (2023). Internal audit function and investment efficiency: Evidence from public companies in Indonesia. Cogent Business and Management, 10(2). https://doi.org/10.1080/23311975.2023.2242174.
5. Babiker I. (2025). The role of internal audit in enhancing cyber security from the auditors' point of view. Journal of Business and Environmental Sciences, 4(1), 127-146
6. Babiker. I(2024):" The Role of Internal Audit in Enhancing Cyber Security From The Auditors' Point of View" Journal of Business and Environmental Sciences Volume: 4(1), Page: 127-146 https://doi.org/10.21608/jcese.2024.321691.1079.
7. Beredugo S. B(2024), "Cyber security Audits And The Mitigation Of CyberAttacks Of Selected Companies In Nigeria", International Journal of EGovernment & E-Business Research, Vol. 9, Issue 1, 2024, pp 19-35, DOI: https://doi.org/10.53882/IJEGEBR.202 4.0901003.
8. Dambe. S, Gochhait. S(2024):" The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit". https://www.researchgate.net/publication/378479488_The_Role_of_Artificial_Intelligence_in_Enhancing_Cybersecurity_and_Internal_Audit?enrichId=rgreq-3aad25aa317f48ccc578a4c8428c7dc0-XXX&enrichSource=Y292ZXJQYWdlOzM3ODQ3OTQ4ODtBUzoxMTQzMTI4MTIyNTc3NDI5NEAxNzA4OTE0NDU4Njgy&el=1_x_2&_esc=publicationCoverPdf.
9. Dikokoe.t(2021):" Role of Internal Audit in Managing Cyber Security Risks". Submitted in fulfilment of the requirements for the degree MAGISTER COMMERCII in COMPUTER AUDITING In the COLLEGE OF BUSINESS AND ECONOMICS at the UNIVERSITY OF JOHANNESBURG.
10. European Confederation of Institutes of Internal Auditors (2020), "Risk in focus 2021. Hot topics for internal auditors", available at: https://www.eciia.eu/wp.
11. Gogineni , S(2023):"Innovative Approaches to Risk Governance Integrating Security Audits with Advanced Cybersecurity Strategies" Economic Sciences https://economic-sciences.com ES (2023) 19(1), 29-42 | ISSN:1505-4683.
12. Hidayat, V. K., & Wang, G. (2023). A Comprehensive Cybersecurity Maturity Study for Nonbank Financial Institution. Journal of System and Management Sciences, 13(5). https://doi.org/10.33168/JSMS.2023.0534.
13. I.Atoum, A. Otoom, and A.A. Ali. "A holistic cyber security implementation framework." Information Management & Computer Security (2014). https://www.researchgate.net/profile/IssaAtoum/publication/265969549_A_holistic_cyber_security_implementation_framework/links/546f49da0cf24af340c08147/A -holistic-cyber-security-implementation-framework.pdf [
14. Innovative Approaches to Risk Governance Integrating Security Audits with Advanced Cybersecurity Strategies Sneha Gogineni USA. Economic Sciences https://economic-sciences.com ES (2023) 19(1), 29-42 | ISSN:1505-4683.

15. Institute of Internal Auditors (IIA) (2020a), "Rethinking preparedness: Pandemics and cybersecurity", available at: https://global.theiia.org/knowledge/Public% 20Documents/IIA-Bulletin-Rethinking-Preparedness-Pandemics-and-Cybersecurity.pdf (accessed 15 October 2020).
16. Johnson K, Cavalli L. AI and automation in internal audits. Technology in Governance. 2023;15(4):90–105. Mbah GO. The Role of Artificial Intelligence in Shaping Future Intellectual Property Law and Policy: Regulatory Challenges and Ethical Considerations. Int J Res Publ Rev. 2024;5(10):[pages unspecified]. DOI: https://doi.org/10.55248/gengpi.5.1024.3123
17. Kotb, A., Elbardan, H., & Halabi, H. (2020) "Mapping of internal audit research: a post-Enron structured literature review", Accounting, Auditing & Accountability Journal, vol. 33, no. 8:1969-1996.
18. L., Joel. "Cybersecurity governance: The role of the audit committee and the CPA." The CPA Journal 84, no. 11 (2014): 6.
19. Lenning, J., & Gremyr, I. (2021) "Unleashing the potential of internal audits: a review and research agenda", Total Quality Management & Business Excellence, vol. 33, no. 9-10:994-1010.
20. Najm . K,Al-Karaawi.(2024)" The role of internal audit commitment in reducing cybersecurity risks "International Journal of Applied Engineering & Technology, Vol. 6 No.1, January, 2024.
21. P. Rosati, F. Gogolin, and T. Lynn. "Cyber-security incidents and audit quality." European Accounting Review (2020): 1-28. http://doras.dcu.ie/25939/1/Rosati%20et%20al.%20%282020 %29%20-%20Cybersecurity%20Incidents%20and%20Audit%20Quality%20- %20Final%20Version.pdf.
22. Rofi'ah, D. M. (2025). NIST Cyber security Framework in the Lens of Indonesian Internal Auditors. Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE), 8(2), 3349–3367. https://ejournal.uac.ac.id/index.php/iijse/article/view /6027.
23. Sarens G, De Beelde I. Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. Managerial Auditing Journal. 2006 Jan 1;21(1):63-80.
24. Sharton, Brenda B. R. (2020), "Will Coronavirus Lead to More Cyber Attacks?" available at: https://hbr.org/2020/03/will-coronavirus-lead-to-more-cyber-attacks? autocomplete=true (accessed 20 October 2020).
25. Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, 33(4). https://doi.org/10.1108/MAJ-07-2017-1596.
26. Taheri, R(2022) : "The Role of Internal Auditing in Activating Risk Management within Algerian Economic Institutions: Case study of Fental Corporation – Tiaret" - p. 50.
27. Tamimi, O. (2021) "The role of internal audit in risk management from the perspective of risk managers in the banking sector", "Australasian Accounting Business and Finance Journal", vol. 15, no. 2:114-129.
28. the auditors' point of view. Journal of Business and Environmental Sciences, 4(1), 127-146
29. Turetken, O., Jethefer, S., & Ozkan, B. (2020) "Internal audit effectiveness: operationalization and influencing factors", Managerial Auditing Journal, vol. 35, no. 2:238-271
30. Udoh . O. R ,Odion.O (2024):" Leveraging technology in internal audit processes for streamlined management and risk oversight" International Journal of Science and Research Archive, 2024, 13(02), 3077-3100.
31. Usman, A., Che-Ahmad, A., Abdulmalik, S. O. (2023) The Role of Internal Auditors Characteristics in Cybersecurity Risk Assessment in Financial-Based Business Organisations: A Conceptual Review. Intern. Journal of Profess. Bus. Review. |Miami, v. 8 | n. 8| p. 01-31 | e02922 | 2023.
32. Usman, A., Elaigwu, M., & Rofeekat, K. (2021). The Role of Internal Audit Function on Cybersecurity Risk Mitigation among Listed Financial Companies in Nigeria: A Conceptual Review Creative Business Research Journal, 1(2), 205-212
33. Vuko. T, Čular. M, Drašček . M, SLAPNIČAR. S (2021):" Key Drivers of Cybersecurity Audit Effectiveness: a neo-institutional perspective. https://www.researchgate.net/publication/355201244_Key_Drivers_of_Cybersecurity_Audit_Effectiveness_a_neo-institutional_perspective?enrichId=rgreq-632ab4d376da070c1e73b344984ca450-XXX&enrichSource=Y292ZXJQYWdlOzM1NTIwMTI0NDtBUzoxMDc4NjUwMTIwMjE2NTgwQDE2MzQxODE2Mzc2NDY%3D&el=1_x_2&_esc=publicationCoverPdf.
34. Williams P. Digital transformation and auditing efficiency. Audit Practices Journal. 2023;11(5):150–165 .

AUTHORS

Dr. Basheer wakas

PhD in Accounting -Accounting Department- Faculty of Economics-Damascus University