THE EXTENT OF EMERGING COMMERCIAL BANKS COMMITMENT TO CYBERSECURITY GOVERNANCE: AN EMPIRICAL STUDY

Aiman Mahmoud Abu Hamour *

* Accounting and Accounting Information System Department, Amman University College for Financial and Managerial Science, Al-Balqa Applied University, Amman, Jordan
Contact details: Accounting and Accounting Information System Department, Amman University College for Financial and Managerial Science, Al-Balqa Applied University, P.O. Box 45, 11831 Amman, Jordan

OPEN ACCESS

How to cite this paper: Hamour, A. M. A. (2023). The extent of emerging commercial banks commitment to cybersecurity governance: An empirical study. *Corporate Governance and Organizational Behavior Review, 7*(2), 111–117.
https://doi.org/10.22495/cgobrv7i2p9

ISSN Online: 2521-1889
ISSN Print: 2521-1870

Received: 26.06.2022
Accepted: 24.03.2023

JEL Classification: M1, M2, M4
DOI: 10.22495/cgobrv7i2p9

Abstract

The interest of business organizations and banks in cybersecurity has become extremely important, and this is evident through many studies such as (Abu-Shanab et al., 2013; Al-Muhtadi, 2020) which emphasized the importance of cybersecurity in business. The study aims to identify the extent of the commitment of Jordanian commercial banks to the governance of cybersecurity, from the point of view of a certified public accountant. However, the population consisted of Jordanian commercial banks, and a sample of 83 respondents was taken from auditors who hold a chartered accountant certificate and work in the field of auditing the accounts of Jordanian commercial banks. The findings indicate that Jordanian commercial banks are committed to cybersecurity governance with regard to cybersecurity governance strategy, cybersecurity related to human resources, and cybersecurity risk management from the point of view of a certified public accountant. Nevertheless, this paper contributes to providing useful results for financial managers and accountants working in Jordanian commercial banks by introducing them to the importance of cybersecurity governance. Through its theoretical literature, prior investigations, and research methodologies whose validity and reliability have been proven and may be employed and used in future studies, it is hoped that this study would motivate many researchers to conduct more new research on this subject.

Keywords: Cybersecurity Governance, Certified Public Accountant, Jordanian Commercial Banks

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

Acknowledgments: This research was funded by the Deanship of Scientific Research and Innovation, Al-Balqa Applied University, Jordan.

1. INTRODUCTION

Cybersecurity is one of the most prominent concepts introduced by the information revolution and the Internet to the operations carried out by organizations, which emerged as a result of technological developments, cyber risks resulting from the possibility of threats and risks in the information technology environment, and cybersecurity expresses a radical shift in concepts

concerned with providing Means, policies, instructions, and practices related to the protection of information. In addition, cybersecurity governance requires an increased capacity to adequately protect the information held by cyberspace organizations against cyberspace threats and risks, and therefore, the cybersecurity governance perspective is the procedures and arrangements for the use of technology that helps secure that protection. This type of governance is the future, as many organizations strive to implement the management of cyber risk, they are likely to be exposed (Grant & Chau, 2005; Abu-Shanab et al., 2013; Al-Ateeq et al., 2022).

Financial and accounting systems, as well as the disclosure and transparency processes in businesses, have all been impacted by the usage of information technology and cyberspace, and the obligation to enter this space into the performance of various types of operations. Concepts of cybersecurity governance that guide, when displaying company achievements in the information technology environment, guidelines and regulations for handling financial and accounting systems have arisen. In addition, the growing use of information technology and the proliferation of cybersecurity have led to more risks and threats. The use of this space has also revolutionized the world of communications, contributing to increasing the risks and threats to which Jordanian commercial banks can be exposed when disclosing their information and data in their financial statements and more efficiently than usual methods of conventional disclosure.

The main problem arises in the technological challenge in cyberspace that requires Jordanian commercial banks to confront it through the governance of cybersecurity, as it is an effective tool that provides the required protection from the attacks that may be exposed to it in this space, which has become very significantly affecting the orbit of integration and homogeneity with the development of technologies Information and communications and their legal requirements, especially since cyber-attacks target financial and banking institutions as an attractive target for these complex programs. Thus, this study aims to reveal the extent of the commitment of Jordanian banks to cybersecurity governance from the point of view of a certified public accountant.

This paper was divided after the introduction section as follows. Section 2 identified the literature review and reported on the development of hypotheses. Section 3 derived the hypotheses of the study. Section 4 presented information about the methodology. Section 5 included the results of the study. Section 6 dealt with the discussion, and finally, Section 7 concluded the paper conclusion.

2. LITERATURE REVIEW

2.1. Cybersecurity governance

The degree of organizations' commitment to applying the general framework for information technology governance has become one of the most important basic criteria that investors consider when making their investment decisions, especially in light of economic globalization and the intensification of competition between different organizations to enter the financial markets, whether local or global, for investment (Solomon et al., 2003; Vito et al., 2022).

Hence, organizations that apply information technology governance and cybersecurity governance have a competitive advantage to attract capital over those that do not apply them, and their competitiveness increases in the long run through the transparency enjoyed by these organizations in their transactions, accounting, and financial audit procedures, and all operations of the organization in a way that supports confidence on the part of investors, whether local or international, to invest in these organizations, and this may lead to a reduction in the cost of capital and may eventually lead to more stability of funding sources (Freeland, 2018).

The researcher believes that cybersecurity governance means reviewing the processes related to implementing cyber risk management resulting from the possibility of risks occurring in the information technology environment in which Jordanian commercial banks operate, thus achieving justice and transparency, granting the right to accountability, and the necessary protection for owners, shareholders, workers, and work interests; reducing misuse of power in ways that are not in the public interest; promoting the development and growth of investments and the promotion of their flows; promoting the development of savings; maximizing profitability; and creating new job possibilities. There are administrative procedures in place that allow management to be held accountable to shareholders.

The following is a review of the three standards related to the general work of cybersecurity governance contained in the instructions for adapting to cyber risks issued by the Central Bank of Jordan in 2018 to audit cyber risks in information technology, as the presence of these frameworks in cybersecurity governance and organizational structure contributes to laying the foundations and appropriate standards. This helps the board of directors to perform the tasks and responsibilities assigned to them at the level of planning for electronic services in the virtual space, leading to the implementation of these tasks and responsibilities and publishing them, measuring the success rate of these services and achieving maximum satisfaction of the target audience. Below is a summary of it.

2.1.1. Cybersecurity governance strategy

The use of information technology gives sufficient opportunity to implement governance procedures with the required speed and accuracy, and organizations' use of information technology enables them to be effective and distinguished. They are supposed to identify a distinct group of information technology that is unique to them to form competitive advantages that contribute to achieving high-performance results (Detlor et al., 2010). Hence, the business technology strategy imposed a new reality as a result of the organizations' activities and transactions' reliance on this technology, which led to the necessity of keeping pace with this development and the importance of changing their traditional methods with innovative methods that depend on modern technological

methods and advanced analytical methods to carry out business efficiently and effectively (Abu-Shanab et al., 2013; Alqaraleh et al., 2022).

The success in implementing the cybersecurity strategy related to the provision of electronic services is ensured, and after these services are subjected to an information effort examination, this strategy is launched and announced via the Internet (Von Haldenwang, 2004). It is worth noting that the administration cannot apply the cybersecurity governance strategy and any electronic services on its portal without the management's approval because this would enhance performance efficiency and accuracy, reduce the time and cost required to complete transactions, ensure integration and coordination between different departments and sections, and achieve efficiency, transparency, and better performance levels (Al-Muhtadi, 2020).

The researcher believes that the cybersecurity governance strategy means the provision of electronic services and is clarified to the beneficiaries and employers to enable them to achieve maximum benefit from the application of the cybersecurity governance strategy and to indicate the extent of the ability to exploit the opportunities available to it in the external environment to obtain scarce resources of value for its continuity. In performing its tasks and activities to achieve its planned goals and objectives, in addition to this, the cybersecurity governance strategy is explained from a technical point of view in order to enable those in charge of developing electronic services to make good use of these services within their approved software. Then it becomes possible to prepare the technical guide for the short guide. For the beneficiaries of the implementation of the cybersecurity governance strategy and the services associated with it, which must be done easily and securely, because there is transparency to track performance and provide knowledgeable information to the decision-maker.

2.1.2. Cybersecurity related to human resources

This framework is represented by the types of qualified and trained human resources in the field of information technology who are able to deal with cybersecurity risks, workers specialized in the implementation of data collection and analysis operations, program designers, device and equipment operators, and maintenance workers, whether related to software maintenance or hardware maintenance, as information technology depends. Communications and cybersecurity greatly affect human thought, which gives them great importance in developing human resources and building the so-called intellectual capital that is adaptable to changes, conditions, and advanced technology (Zahlan, 2019).

Freeland (2018) believes that the importance of human resources in information technology increases with the increase in information available to the organization in making a specific decision, which requires it to pay attention to an important and significant aspect of how to transform this enormous information into knowledge and determine the places and timing of its use, and this, In turn, it requires advanced information technology in a way that allows it to be logically interconnected, and within this framework (Moynihan, 2014), it indicates that the board of directors uses some qualified and sufficiently trained employees in information technology and cybersecurity related to human resources to perform some tasks and responsibilities such as government procedures engineer, electronic services programming expert, web services confidentiality and security expert, human and financial resources systems expert, and electronic broker expert.

The researcher considers that cybersecurity is related to human resources means that Jordanian commercial banks provide human resources and manpower in information technology who are able to use electronic systems so that they have sufficient skill in the use of computer hardware and software in order to perform the specific tasks and duties entrusted to them because information and communication technology depend in a great way on these resources.

2.1.3. Cybersecurity risk management

Managing cybersecurity threats necessitates preserving the network's data security. To access the network, the user needs a unique account. No one is allowed to enter the network unless they have an account name and a particular password that allows them to access the data of the company (Al-Khalidi, 2015; Al-Zaqeba et al., 2018, 2022). Thus, in addition to the industry's slow modernization and development, risks that prevent the implementation of cybersecurity governance include failure to ensure the privacy of information and data available within the electronic network, worry about information leakage that the owner does not want others to know, and a lack of programs to encrypt the information that must be transferred in order to maintain the required security and confidentiality (Al-Muhtadi, 2020; Dahiyat, 2022).

By securing and maintaining the privacy and confidentiality of data from threats or attacks, as well as by providing the tools and means to protect data from internal threats, the cybersecurity risk management strategy is a technique for using information technology to prevent the penetration of an accounting system on the Internet. Or external, as access to the Internet requires a specific account, and no one is permitted to enter the network or use a company's data without entering their account name and password. Information security is crucial for both of these reasons (Laudon & Laudon, 2018).

The researcher believes that there are aspects that require study and research in managing cybersecurity risks in light of the use of the Internet and the existence of a set of methods to penetrate the information system, in addition to the violation of the intellectual rights of individuals and organizations in the electronic world.

2.2. Certified public accountant's relationship with cybersecurity governance

For the profession of accounting and auditing to be successful in providing services to all parties with an interest in the profession's outputs, it relies on the public's trust. In order to benefit from it in making decisions, the role of the certified public accountant in applying cybersecurity governance has emerged as an important, necessary, and desired

goal in terms of including that governance of the aspects that prevent users from misleading it from different groups of society (Al-Jaafari, 2015).

The report presented by the certified public accountant is one of the most important means and methods used by the administration through cybersecurity governance for the purpose of verifying the quality of financial reports, and it is one of the control loops that provide the administration with continuous information. The function of the certified public accountant plays an important role in improving the quality of financial reports, as it enhances this process, as the certified public accountant, through the activities he carries out, increases credibility, and fairness, and reduces risks, as the certified public accountant is an important mechanism of control within the framework of the cybersecurity governance structure, particularly concerning ensuring the accuracy and integrity of financial reports and statements (Archambeault, 2020).

Most users of reports and financial statements rely heavily on appropriate and reliable information so every decision-maker in buying, selling, or keeping investment tools needs reliable information to make rational decisions. Providing impartiality in accounting information about price fairness, as care must be taken to ensure that the accounting information shows the reality of the situation of the organization that issues the data, as it is not in a way that achieves the desire of a particular group (Marston, 2003; Al-Zaqeba et al., 2022).

This leads to achieving cybersecurity governance in a manner that determines the value of the benefit to the user of accounting information, which helps decision-makers to rely on this data, as well as the period and timing of publishing this data and information so that any delay in the audits will affect the time of publishing this information, and this is confirmed by the importance of planning and completing the operations of the certified public accountant by issuing the report that contains his/her opinion (Solomon et al, 2003; Al-Zaqeba & Al-Rashdan, 2020b). However, the main function of a certified public accountant is to give confidence to the financial statements and reports and the information they contain and to contribute to providing appropriate and reliable financial information to its users and protecting users of this information. This requires the certified public accountant to enjoy the confidence of others who depend on his/her opinion as an expert judge in the fairness of representing the financial statements. In order to achieve this goal, it is assumed that the beneficiaries who depend on the opinion of the certified public accountant have a high degree of confidence in that opinion.

3. HYPOTHESIS DEVELOPMENT

Bierstaker et al. (2001) concluded that the shift from paper systems to advanced audit programs led to the completion of the application of most audit procedures, and that information technology governance has a significant impact on the stages of the audit process and allows auditing all client data. This in turn will lead to huge gains in audit efficiency and effectiveness. the accounts.

Nassour (2015) recommends the necessity of applying a model to control information technology in the banks under study, and to be a tool for preparing financial statements and reports in a way that reflects positively on the reliability of this information and increases the confidence of investors who deal with these banks.

Bahl and Wali (2014) showed that companies that provide information technology outsourcing services in India and that provide software services have an important and fundamental impact on service quality and information security that can be predicted, and it was found that there is a positive impact relationship between the elements of security governance in information technology and the quality of information security services provided by information technology (IT) outsourcing companies in India. It recommended the need to organize training courses on how to create software services related to the governance of information technology security because of its impact on the quality of service and information security that companies provide to clients benefiting from their services in India.

Gary (2016) confirms that senior management and boards of directors ensure the security and protection of information in their organizations and always research this matter and put it on the priority list of their work. The study recommended the necessity of creating information technology governance legislation to alleviate the concerns of investors, users, organizations, and customers over the security and confidentiality of information in organizations.

Through a field study of Egyptian companies and banks operating in the virtual village, El-Maghrabi et al. (2018) aimed to identify the impactful role of information security governance in reducing the risks of accounting information systems. A survey list was used to collect information from the study sample, which amounted to 125 financial managers and accountants working in Egyptian companies. The questionnaire data were analyzed using means and standard deviations. The study showed a significant impact of the application of information security governance standards in reducing the risks of accounting information systems in Egyptian companies, and it was found that there are a number of risks to which electronic accounting information systems are exposed, including external risks as a result of threats in the electronic business environment, and the study recommended the need for companies and banks to The Egyptian woman who works in the virtual village is interested in preparing information technology guides and paying attention to modern methods of measuring and evaluating performance in the company.

Slupska (2021) dealt with cybersecurity governance as one of the terms used to describe and understand new technologies that require adherence to ethics and adequate protection of information owned by organizations from cyber threats and risks in cyberspace. This study is considered one of the descriptive theoretical studies that talked about cybersecurity governance, which bears a set of assumptions about roles and moral obligations to deal with cybersecurity problems, which is called a metaphor of electronic warfare that reduce

the possibilities of international cooperation in this field by limiting countries to taking reactive policies and taking proactive measures to address the features and characteristics of financial systems in the cyberspace The study recommended the use of alternative metaphors such as health, ecosystem, and architecture that can help provide more cooperation and apply the nuanced conceptual framework for negotiations to implement the management of cyber risks that they are likely to be exposed to.

Thus, the following hypotheses are proposed:

H1: Jordanian commercial banks are not committed to the governance of cybersecurity from the point of view of the certified public accountant.

H1a: Jordanian commercial banks do not adhere to the cybersecurity governance strategy from the point of view of the certified legal accountant.

H2b: Jordanian commercial banks are not committed to cybersecurity related to human resources from the point of view of the certified public accountant.

H3c: Jordanian commercial banks are not committed to managing cybersecurity risks from the point of view of a certified public accountant.

4. RESEARCH METHODOLOGY

This paper relied on the use of a descriptive and analytical approach, through a field survey of the Jordanian commercial banking community. The study population consists of all certified Jordanian accountants in Jordan.

The questionnaire was developed by referring to previous relevant studies, and the items in the previous studies, after their modification, were translated into Arabic, which is the main language in Jordan, to ensure the participation of the largest possible number of respondents.

Studies by Slupska (2021) and Bahl and Wali (2014) were used to develop the measurement methods used in the questionnaire.

The validity of the content was confirmed by presenting the questionnaire to a group of academics specialized in accounting science, where all their requested amendments were taken.

The reliability of the questionnaire was verified by conducting a pilot study on 25 accountants from outside the actual study sample, and the questionnaire's stability was higher than 0.70, this indicates the verification of reliability. After distributing the questionnaire, the reliability of the questionnaire was verified by calculating Cronbach's alpha values, which amounted to 0.902, meaning that it is higher than 0.70, and therefore it can be said that the reliability was achieved in this study (Hair et al., 2019).

To achieve the objectives of the study, the type of study sample was determined according to the appropriate sample, as it is difficult to conduct random sampling because of the specificity of the study sample in terms of functional and demographic features.

The study sample was selected from auditors who have a chartered accountant certificate and who work in the field of auditing the accounts of Jordanian commercial banks, whether they are internal or external auditors of the bank. The appropriate sample size was 100 questionnaires distributed to them, and 83 questionnaires were retrieved, accounting for 86% of the total questionnaires sent. They were subjected to statistical analysis.

5. FINDINGS

The results of the descriptive analysis of the study sample showed that cybersecurity governance is of high importance and that the study sample members have a high interest in cybersecurity related to human resources and cybersecurity risk management.

The following tables show the results that were reached in testing the hypotheses of the study (Hair et al., 2019), from the point of view of the certified public accountant, and they were as follows (see Table 1).

Table 1. Results of t-test analysis

Variable	*Mean*	*Std. dev.*	*Calculated t-value*	*Tabular t-value*	*Sig.**	*Result*
The extent of Jordanian commercial banks' commitment to cybersecurity governance	3.740	0.5924	15.22	1.673	0.000	Rejection of the nihilistic hypothesis
The extent of Jordanian commercial banks' commitment to the cybersecurity governance strategy	3.729	0.5573	11.95	1.673	0.000	Rejection of the nihilistic hypothesis
The extent to which Jordanian commercial banks are committed to cybersecurity related to human resources	3.732	0.5794	12.65	1.673	0.000	Rejection of the nihilistic hypothesis
The extent to which Jordanian commercial banks are committed to managing cybersecurity risks	3.765	0.5429	16.81	1.673	0.000	Rejection of the nihilistic hypothesis

*Note: * significant at the 0.05 level*

It is clear from the data in the previous table that the calculated level of significance (Sig.) reached 15.22 to the extent of Jordanian commercial banks' commitment to cybersecurity governance, the calculated level of significance reached 11.95 to the extent of Jordanian commercial banks' commitment to the cybersecurity governance strategy. Also, it is clear from the data that the calculated level of significance reached 12.65 the extent to which Jordanian commercial banks are committed to cybersecurity related to human resources, and the calculated level of significance reached 16.81 the extent to which Jordanian commercial banks are committed to managing cybersecurity risks, and by comparing the values that were reached in testing hypothesises, the null hypothesises are rejected.

The results of the survey indicate that Jordanian banks focus largely on introducing cyber security strategies into their banking operations and

activities, as well as introducing security-supported financial technology to protect the privacy and confidentiality of customers.

In addition, Jordanian banks are adopting the introduction of artificial intelligence techniques to improve cybersecurity, as these technologies help financial managers to manage risks efficiently, thus enhancing the level of cybersecurity within these banks.

6. DISCUSSION

The main objective of this paper was to reveal the extent of Jordanian banks' commitment to cybersecurity governance from the point of view of a certified legal accountant. It was found that Jordanian commercial banks adhere to the cybersecurity governance strategy. This finding was consistent with the study of Bierstaker et al. (2001), as well as adhering to human resources cybersecurity. It was found that basic training materials are being audited through which workers' cybersecurity policies and procedures are communicated. This finding agreed with a study (Bahl & Wali, 2014), which recommended the need to organize training courses on how to find software services related to IT security governance. The results indicated that it was committed to managing cybersecurity risks, and the bank's management was found to exercise its supervisory and oversight role in determining cybersecurity risks. This result was consistent with the study (Nassour, 2015), and the documents were audited to ensure that cybersecurity risks were part of the IT governance framework.

According to the results of this study, the managers of Jordanian commercial banks should focus greatly on adopting modern financial technology that guarantees privacy and security for customers in banking transactions and providing a strong infrastructure that can be used to enhance cybersecurity, and this improves the level of security in general, leading to the achievement of competitive advantages. These new banks help them increase profitability in the short, medium, and long term.

7. CONCLUSION

This study aims to identify the extent of the commitment of Jordanian commercial banks to the governance of cybersecurity, from the point of view of a certified public accountant

The study reached a set of interesting results, as it was confirmed that Jordanian commercial banks are committed to cybersecurity governance with regard to cybersecurity governance strategy, cybersecurity related to human resources, and cybersecurity risk management from the point of view of a certified public accountant.

The results indicate that Jordanian commercial banks are committed to the governance of cybersecurity from the point of view of the certified public accountant, and this paper contributes to providing useful results for Jordanian financial managers and accountants working in commercial banks by introducing them to the importance of cybersecurity governance. Through its theoretical literature, prior investigations, and research methodologies whose validity and reliability have been proven and may be employed and used in future studies, it is hoped that this study would motivate many researchers to conduct more new research on this subject.

Where this study calls for future studies to increase interest in the factors affecting cyber security and the factors affecting the dependence of accountants and financial managers on advanced accounting information systems, which focus on the use of advanced electronic means of protection.

This study also invites researchers to study other variables that may contribute to understanding the enabling factors of cybersecurity in addition to improving financial performance.

REFERENCES

1. Abu-Shanab, E. A., Harb, Y. A., & Al-Zoubi, S. Y. (2013). E-government as an anti-corruption tool: Citizens perceptions. *International Journal of Electronic Governance, 6*(3), 232–248. https://faculty.yu.edu.jo/emad/Lists/Published%20Research/Attachments/29/Abu-Shanab-Harb-Al-Zoubi-2013.pdf
2. Al-Ateeq, B., Sawan, N., Al-Hajaya, K., Altarawneh, M., & Al-Makhadmeh, A. (2022). Big data analytics in auditing and the consequences for audit quality: A study using the technology acceptance model (TAM). *Corporate Governance and Organizational Behavior Review, 6*(1), 64–78. https://doi.org/10.22495/cgobrv6i1p5
3. Al-Jaafari, W. (2015). *The auditor's role and responsibility in meeting the needs of users of financial statements.* Arab Institute of Certified Public Accountants.
4. Al-Khalidi, N. (2015). The impact of using electronic data processing methods on increasing the effectiveness of audit offices operating in the Gaza strip. *Scientific Journal, 23*(1), 282–304.
5. Al-Muhtadi, S. Z. (2020). *Electronic governance technology.* Osama House for Publishing and Distribution.
6. Alqaraleh, M. H., Almari, M. O. S., Ali, B. J. A., & Oudat, M. S. (2022). The mediating role of organizational culture on the relationship between information technology and internal audit effectiveness. *Corporate Governance and Organizational Behavior Review, 6*(1), 8–18. https://doi.org/10.22495/cgobrv6i1p1
7. Al-Zaqeba, M. A. A. (2019). *Tax compliance behavior among high income individual taxpayers in Jordan: The moderating effect of trust and religiosity* [Doctoral dissertation, Universiti Sains Islam Malaysia]. https://oarep.usim.edu.my/jspui/handle/123456789/6410
8. Al-Zaqeba, M. A. A., & Al-Rashdan, M. T. (2020a). Extension of the TPB in tax compliance behavior: The role of moral intensity and customs tax. *International Journal of Scientific & Technology Research, 9*(4), 227–232. https://www.ijstr.org/final-print/apr2020/Extension-Of-The-Tpb-In-Tax-Compliance-Behavior-The-Role-Of-Moral-Intensity-And-Customs-Tax.pdf
9. Al-Zaqeba, M. A. A., & Al-Rashdan, M. T. (2020b). The effect of attitude, subjective norms, perceived behavioral control on tax compliance in Jordan: The moderating effect of costums tax. *International Journal of Scientific & Technology Research, 9*(4), 233–238. https://www.ijstr.org/final-print/apr2020/The-Effect-Of-Attitude-Subjective-Norms-Perceived-Behavioral-Control-On-Tax-Compliance-In-Jordan-The-Moderating-Effect-Of-Costums-Tax.pdf

10. Al-Zaqeba, M. A. A., Hamid, S. A., & Muhammad, I. (2018, April 22–23). Tax compliance of individual taxpayers: A systematic literature review. In *Proceedings of the IIER International Conference* (pp. 42–52). https://www.researchgate.net/publication/335704083_TAX_COMPLIANCE_OF_INDIVIDUAL_TAXPAYERS_A_SYSTEMATIC_LITERATURE_REVIEW
11. Al-Zaqeba, M. A. A., S, A. H., Ineizeh, N. I., Hussein, O. J., & Albawwat, A. (2022). The effect of corporate governance mechanisms on earnings management in Malaysian manufacturing companies. *Asian Economic and Financial Review, 12*(5), 354–367. https://doi.org/10.55493/5002.v12i5.4490
12. Archambeault, D. S. (2020). *The relation between corporate governance strength and fraudulent financial reporting: Evidence from SEC enforcement cases* (Working Paper). School of Business.
13. Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security, 22*(1), 2–23. https://doi.org/10.1108/IMCS-01-2013-0002
14. Bierstaker, J., Burnaby, P., & Thibodeau, J. (2001). The impact of information technology governance on the audit process: An assessment of the state of the art and implications for the future. *Managerial Auditing Journal, 16*(3), 159–164. https://doi.org/10.1108/02686900110385489
15. Dahiyat, A. (2022). Robotic process automation and audit quality. *Corporate Governance and Organizational Behavior Review, 6*(1), 160–167. https://doi.org/10.22495/cgobrv6i1p12
16. Detlor, B., Hupfer, M. E., & Ruhi, U. (2010). Internal factors affecting the adoption and use of government websites. *Electronic Government, an International Journal, 7*(2), 120–136. https://doi.org/10.1504/EG.2010.030923
17. El-Maghrabi, M. H., Gable, S., Osorio Rodarte, I., & Verbeek, J. (2018). *Sustainable development goals diagnostics: An application of network theory and complexity measures to set country priorities* (Policy Research Working Paper No. 8481). World Bank. https://ssrn.com/abstract=3238315
18. Freeland, C. (2018, May 7–8). *Basel committee guidance on electronic corporate governance for banks* [Paper presentation].
19. Grant, G., & Chau, D. (2005). Developing a generic framework for e-government. *Journal of Global Information Management, 13*(1), Article 1. https://doi.org/10.4018/jgim.2005010101
20. Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203
21. Ineizeh, N. I., Al-Zaqeba, M. A. A., Hussein, O. J., & Yamin, I. Y. (2022). Corporate social responsibility disclosure by Islamic banks in GCC region. *Universal Journal of Accounting and Finance, 10*(2), 707–718. http://doi.org/10.13189/ujaf.2022.100308
22. International Arab Society of Certified Accountants (ASCA). (2011). *International financial reporting standards.*
23. Jarah, B. A. F., Al-Jarrah, M. A. A., & Al-Zaqeba, M. A. A. (2022). The role of internal audit in improving supply chain management in shipping companies. *Uncertain Supply Chain Management, 10*, 1023–1028. https://doi.org/10.13189/ujaf.2022.100308
24. Laudon, K. C., & Laudon, J. P. (2018). *Essentials of management information systems* (13th ed.). Pearson.
25. Malkawi, R., Alzaqebah, M., Al-Yousef, A., & Abul-Huda, B. (2019). The impact of the digital storytelling rubrics on the social media engagements. *International Journal of Computer Applications in Technology, 59*(3), 269–275. https://doi.org/10.1504/IJCAT.2019.098605
26. Marston, C. (2003). Financial reporting on the internet by leading Japanese companies. *Corporate Communication: An International Journal, 8*(1), 23–34. https://doi.org/10.1108/13563280310458894
27. Nassour, R. (2015). *The impact of information technology governance on the quality of financial reports: A field study* [Doctoral dissertation, Tishreen University].
28. Qasim, Y. R., Ibrahim, N., Sapian, S. B. M., & Al-Zaqeba, M. A. A. (2017). Measurement the performance levels of Islamic banks in Jordan. *Journal of Public Administration and Governance, 7*(3), 75–87. https://doi.org/10.5296/jpag.v7i3.11451
29. Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Wiley.
30. Slupska, J. (2021). War, health and ecosystem: Generative metaphors in cyber security governance. *Philosophy & Technology, 34*, 463–482. https://doi.org/10.1007/s13347-020-00397-5
31. Solomon, J. F., Lin, S. W., Norton, S. D., & Solomon, A. (2003). Corporate governance in Taiwan: Empirical evidence from Taiwanese company directors. *Corporate Governance: An International Review, 11*(3), 235–248. https://doi.org/10.1111/1467-8683.00321
32. Vito, B., Firmansyah, A., Qadri, R. A., Dinarjito, A., Arfiansyah, Z., Irawan, F., & Wijaya, S. (2022). Managerial abilities, financial reporting quality, tax aggressiveness: Does corporate social responsibility disclosure matter in an emerging market? *Corporate Governance and Organizational Behavior Review, 6*(1), 19–41. https://doi.org/10.22495/cgobrv6i1p2
33. Von Haldenwang, C. (2004). Electronic government (e-government) and development. *The European Journal of Development Research, 16*(2), 417–432. https://doi.org/10.1080/09578810420002208 86
34. Zahlan, A. (2019). *The Arabs and the challenges of science and information technology.* Center for Arab Unity Studies.