IRMM

INTERNATIONAL REVIEW OF MANAGEMENT AND MARKETING

EJ EconJournals
ISSN: 2146-4405

International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2025, 15(3), 398-405.

EJ EconJournals

Exploring the Role of Digital Transformation in Mitigating Accounting Fraud: A Cybersecurity Perspective

Farah Abu-Dabaseh[1], Mohamed Mahmoud Khtatbeh[2]*, Kayed Al'Ararah[3], Abdalla Alassuli[2]

[1]King Abdullah II School of Engineering, Princess Sumaya University for Technology, Jordan, [2]Faculty of Business, Amman Arab University, Jordan, [3]Department of Business Management, Girne American University, North Cyprus Via Mersin 10, Turkey. *Email: m.khtatbeh@aau.edu.jo

Received: 05 December 2024 **Accepted:** 27 March 2025 **DOI:** https://doi.org/10.32479/irmm.18490

ABSTRACT

Artificial intelligence, blockchain, and big data analytics have long disrupted business functions through digital transformation. While these innovations enhance the efficiency of operations and amplify the possibility of fraud detection, they also create avenues for fraud modulation that could conceivably heighten accounting fraud risk. This paper would go deep into how digital transformation influences accounting fraud risks, with a special focus on the role of cybersecurity maturity. Extensive research into the benefits of digitalization has not considered how cybersecurity maturity influences the effectiveness of such technologies in fraud risk mitigation. This study used a quantitative approach based on data collected from 204 employees of audit and accounting firms in Jordan. We assessed the relationship among the constructs using structural equation modeling with partial least squares. The results highlight the significant negative relationship that occurred between the accounting fraud risks and digital transformation, showing that digital technologies decrease fraud vulnerabilities when implemented effectively. Beyond the aforementioned, cybersecurity maturity proved to play a crucial role in moderating and strengthening the ability of digital transformation to mitigate fraudulent cases. These findings underline the need for organizations to go along with technological advancements by implementing appropriate cybersecurity frameworks in order to reap maximum benefits from digital transformation. In this light, the combination of technological innovation with integrated and mature security protocols can help an organization reduce fraudulent risks and work toward strengthening its financial integrity. Thus, this remains a valuable contribution to scholarship, assisting organizations and policymakers in navigating the complexities associated with the dual imperatives of digital transformation and fraud prevention in today's digital era.

Keywords: Digital Transformation, Accounting Fraud Risks, Cybersecurity Maturity, Fraud Mitigation, Financial Integrity, Jordan
JEL Classifications: D81, M15, M41, O33

1. INTRODUCTION

In today's fast-changing business environment, digital transformation is crucial as it changes industries and encourages innovation. Advanced technologies like artificial intelligence (AI), big data analytics, blockchain, and cloud computing have changed how organizations work (Salah and Alzghoul, 2024), especially in accounting and financial management. The modern technologies help organizations run more smoothly, make better decisions, and enhance the accuracy of financial reports (Al Kasasbeh et al., 2023; Alzghoul and Al-kasasbeh, 2024; Putri, 2024). However, the increasing reliance of organizations on digital systems has also led to significant risks, particularly in the realm of accounting fraud. These linked yet segmented systems provide an attacker with vulnerabilities that he can exploit against an organization, thereby posing a threat to its security and financial stability (Daraojimba, 2023; Al-Ghamdi, 2023). Accounting fraud is to be a case of intentional alteration or misrepresentation of facts in financial data presentation. It is one of the frequent problems observed across industries (Ali et al., 2024). Therefore, the transition to digital tools led to an increase in various attack methods, which in turn heightened pressure on organizations to implement robust measures to safeguard their financial systems. Whereas shifting to the realm of digital transformation provides top-notch tools for fraud detection and prevention, it depends on whether effective cybersecurity frameworks are present. Without an effective cybersecurity framework, these systems could unintentionally perpetuate fraud cases, thereby contradicting their intended purpose (Odeyemi et al., 2024; Ridzuan et al., 2022).

This context expects cybersecurity maturity to mediate an organization's ability to withstand cyberattacks, protect its resources, and act efficiently in incidents. Advanced cybersecurity maturity involves obtaining well-defined protocols and having policies of continuous improvement. This will further fortify the strength of online systems and make them more effective in taming fraud risk in the course of transformation toward a digital model (Tam & Jones, 2019). Conversely, low cybersecurity maturity exposes organizations to greater risk of hacker attacks that could significantly influence overall financial and reputational consequences due to fraudulent activities (Alhanatleh et al., 2024; Suela, 2024). The paper investigates the extent to which cybersecurity maturity may moderate the influence of digital transformation on accounting fraud risk. It helps explain how organizations can make better use of facilities provided by digital transformation in view of improving fraud risk mitigation. The study investigates the relationship between technological evolution and its regulatory protection. This research also fills a gap in literature by assessing different influences of cybersecurity maturity on the association between digital transformations and accounting fraud.

2. LITERATURE REVIEW

Digital transformation plays a crucial role in decreasing the risk of accounting fraud through the adoption of state-of-the-art technologies and processes that improve fraud detection, prevention, and organizational resilience (Asad, 2025; Chen et al., 2024; Odeyemi et al., 2024). Digital tools explain the inverse relationship by enhancing internal controls, improving transparency, and promoting real-time monitoring of financial transactions. However, its effectiveness is contingent upon the strategic implementation of digital technologies and appropriate fraud risk management practices (Abousweilem et al., 2023; Alzghoul et al., 2024). Digital transformation integrates digital technologies into all organizational business aspects, radically changing how it operates and generates value (Aboalganam and Alzghoul, 2025). It is evident that tools such as AI, RPA, and blockchain can significantly enhance the organization's ability to detect and prevent fraud. For example, a study by Tiron-Tudor et al. (2022) proves that it is possible to continuously monitor and analyze financial data using such technologies in a way that fraud does not go undetected. Meanwhile, Zhu et al. (2021) presented evidence regarding how deep learning models could extract anomalies in big datasets depicting fraud and underpin the transformational power of digital analytics to prevent fraud.

Other emerging technologies also lie at the very core of forensic accounting, whereby auditors have been able to detect complicated fraud schemes with a higher degree of precision through digital transformation (Roszkowska, 2021). Today, forensic accountants utilize more sophisticated tools in order to analyze data, come up with patterns, and track fraudulent transactions (Ibrahim, and Eriki, 2020). According to Odeyemi et al. (2024), one needs to keep pace with technology in order to be able to fight fraud effectively within the financial world, which has become quite dynamic. The integration of forensic accounting practices with digital tools also enhances internal fraud prevention and detection capabilities. This underscores the inverse relationship between digital transformation and fraud risks, as the approach amplifies the visibility of any fraudulent activity (Bansal et al., 2024). Besides, digital transformation enhances internal controls by automating processes that, in the analogue era, used to be prone to human error or manipulation (Suri, 2022). Blockchain technology, for instance, guarantees data integrity and complete transparency, making it more difficult for fraudsters to tamper with financial records without detection (Dashkevich et al., 2024). According to Tariq et al. (2022), RPA and AI have introduced a number of automated processes that close all the entry points created due to manual intervention. Therefore, these technologies significantly reduce the risks of fraud. These technologies put into place an overall capability to enable an organization to create a strong operational framework that is resistant to fraud.

A third but crucial factor is the role of digital literacy and skill development in the inverse relationship that describes digital transformation in accounting fraud cases (Imjai et al., 2025; Karaki et al., 2023). In this respect, Ridzuan et al. (2022) show that fraud risk assessments are effective due to the digital competencies of auditors and accountants. This will enable organizations to invest in programs that train personnel in the application of digital aids to combat crime. Such a development in human capital supplements technical developments in fraud mitigation. Despite the increased vulnerability resulting from the shift to digital frameworks, nations can still reap benefits from this transformation. While rapid adoption of digital tools introduces new risks, proactive measures in the form of robust cybersecurity frameworks and fostering a culture of digital vigilance go a long way in mitigating them. Goh (2020) has highlighted how anomaly detection is core to visual analytics and data-driven techniques and how an organization needs to take a proactive stance in fraud prevention.

The COVID-19 pandemic shed new light on the inverse relationship between digital transformation and fraud risks. The transition to working from home and changing business models compelled organizations to accelerate their digital initiatives, resulting in increased scrutiny in areas such as internal controls. As such, according to Metwally et al. (2022), only organizations that had already put in place effective digitized solutions were in a better place to mitigate fraud risks and, therefore, had resilience through digital transformation. In respect of the discussion, digital transformation inversely relates to accounting fraud risk because it strengthens an organization's power of detection, obstruction, and resolution of fraudulent activities. Advanced technology, robust internal controls, and fostering digital literacy within an organization can effectively mitigate fraud. These findings from the different studies confirm that strategic use of digital transformation initiatives is important in the protection of financial integrity in the increasingly digital business environment.

H_1: Digital transformation is inversely associated with the risk of accounting fraud.

While there is a significant correlation between digital transformation and accounting fraud risk, the maturity of cybersecurity protocols does significantly moderate this effect. That is, the more organizations are embracing digital transformation and integrating new technologies like AI, RPA, and blockchain, the more they inadvertently set up new vulnerabilities (Putnoki and Orosz, 2023). Considering how important this kind of vulnerability is, it significantly raises regions' risks of accounting fraud, mainly because of poor security measures, as Tiron-Tudor et al. (2022) and Metwally et al. (2022) pointed out. They said that the more businesses digitize, the more they change and become more efficient, but it also makes risk management more difficult in the same place or anywhere else. Although the pace of digital transformation can be rapid, it typically lags behind advancements in cybersecurity. As a result, fraudsters can find many avenues to conduct fraud. While digital ledger technologies empower an organization to enhance data integrity, they may also face heightened risks if cybersecurity protocols fail to keep pace with emerging threats.

Cybersecurity protocol maturity acts as a moderating factor in how well an organization can mitigate such risks. Organizations can use more advanced security measures like real-time monitoring, encryption, and multi-factor authentication (Vance et al., 2023) when they are more mature, according to frameworks like the Cybersecurity Capability Maturity Model (C2M2). Such measures not only help protect sensitive financial information but, at the same time, minimize chances of unauthorized access and fraudulent manipulations (Alfaadhel et al., 2023). Additionally, it is important to consider human elements in cybersecurity maturity. Good cybersecurity awareness and practice among employees add much value to fraud risk mitigation for any organization. A strong cybersecurity culture fosters better compliance by way of frequent training and clear communication, hence minimizing vulnerabilities (Abu-Dabaseh et al., 2024). However, inconsistent use of cybersecurity technologies or conflicts among rules can lead to exploitable weaknesses, underscoring the importance of adopting holistic strategy approaches that encompass both technical and behavioral aspects of cybersecurity. That is, applying holistic strategies integrates both technical and behavioral dimensions about cybersecurity (Pollini et al., 2021).

The COVID-19 pandemic accelerated digital transformation globally, increasing dependence on third-party services and remote work technologies (Alhanatleh et al., 2024). Organizations need to address risks introduced by external dependencies, leading to an increase in demand for mature cybersecurity protocols (Abdel-Rahman, 2023). Mature cybersecurity frameworks enable an organization to implement strict controls, monitor third-party activities, and ensure compliance with security standards, thereby mitigating risks related to outsourcing and remote operations (Metwally et al., 2022). In forensic accounting, cybersecurity protocols would have reached a stage of maturity that complement fraud detection processes. People are increasingly employing advanced technologies that use artificial intelligence and machine learning to detect fraudulent activities (Zhang et al., 2020). These tools shall only be effective if they are premised on secure and reliable data. Gaps in cybersecurity compromise the integrity of data, rendering fraud detection efforts ineffective (Odeyemi et al., 2024). Organizations cannot underestimate the role of mature cybersecurity in supporting the integrity of forensic processes. Secondly, technologies such as blockchain, while offering greater transparency and data security, also introduce new challenges requiring mature cybersecurity responses. An organization with mature cybersecurity protocols will, therefore, be able to exploit the benefits of blockchain by reducing its associated risks, a factor that balances the drive for innovation while keeping security abreast (Tariq et al., 2022).

Regulatory compliance also supports this view of cybersecurity maturity. In recent years, various governments have implemented strict cybersecurity regulations, guiding organizations towards best practices that enhance cybersecurity maturity and deter accounting fraud by enforcing organizational accountability and transparency (AllahRakha, 2024; Saleem et al., 2024). Moreover, cybersecurity protocols play a crucial role in moderating the relationship between digital transformations and accounting fraud risk. The higher the cybersecurity maturity of an organization, the easier it will be to deal with complications brought about by digital transformation, to mitigate emerging risks, and to preserve financial integrity. The best way to handle the connection between digital transformation and fraud risk is to take a proactive, all-encompassing approach that includes cutting-edge technology, strategies that focus on people, and strict adherence to rules.

H_2: The maturity of cybersecurity protocols moderates the relationship between digital transformation and the risk of accounting fraud.

3. RESEARCH METHOD

The study adopts a quantitative research design in investigating the role of digital transformation in reducing accounting fraud, with a focus on the moderating effect of cybersecurity maturity. A quantitative approach is appropriate for this research because it allows for systematic measurement and analysis of relationships between variables. Using structured data collection and statistical analysis, the research design allows for valid investigation of findings, giving us useful information about how digital transformation works and how to stop fraud. This research targets a study population of employees working within audit and accounting companies in Jordan. We designed the sample size to be representative of all categories, using a stratified random sampling approach to capture different hierarchies of employees, jobs, and organizational types. This study's findings will enhance its representativeness by providing a broad range of insights into the auditing and accounting industry. The use of stratification guarantees the variation in the different experiences and practices that epitomize this particular industry; hence, the results would be more generalizable.

Data collection was based on a structured questionnaire with statements related to the variables of interest: digital transformation practices, perceptions of risks of accounting fraud, and levels of cybersecurity maturity. In order to make it easier and more accessible for respondents, we sent an electronic questionnaire by email using Google Forms. Out of 500 invitations, the researchers deemed 204 responses valid, indicating a response rate of approximately 40.8%. The study pretested the questionnaire on a small number of participants before full-scale distribution to ensure its clarity, reliability, and accurate capture of the constructs of interest. The researchers analyzed the collected data using partial least squares-structural equation modeling. The research used this method because it supports complex models with a large number of independent and dependent variables and is robust for small to moderate sample sizes. You can test your ideas about the digitally enabled relationships between accounting fraud risks and cybersecurity maturity using SEM-PLS. In the model fit analysis, reliability and validity supported the robustness of the results.

Given the fundamental nature of the constructs under study, we measured them using well-established scales, which we adapted to better capture digital transformation, accounting fraud, and cybersecurity maturity. We measured the level of digital transformation using an 11-item scale. These factors included the adoption and actual use of advanced technologies such as AI, cloud computing, big data, and their integration with the company's operational processes in a digital mode. The discussion also examined other factors such as innovation, digital culture, employee training programs, and the development of digital skills. The instrument also measured perceived advantages of going digital in terms of enhanced operational efficiency and improved capability for better decision-making. The study measured accounting fraud with an 8-item scale assessing the prevalence, perception, and vulnerability of an organization to fraudulent activities. The items in these scales ranged from perceived awareness of fraud in financial reporting and fraud detection systems to the nature of fraud risk encountered, manipulation, or falsification of data. It also examined employees' perceptions of fraud susceptibility, and the extent of proactive measures implemented for fraud prevention and control. A 14-item scale measured the maturity of cybersecurity, assessing an organization's preparedness through policies and practices against cyber threats. Items ranged in focus from an implementation of the cybersecurity framework and protocol, employee training, and awareness of cyber risk to the advanced use of tools for cybersecurity, such as encryption and firewalls.

4. RESULTS AND DISCUSSION

The measurement model assessment presents the appropriateness, reliability, and validity of the constructs. A sound and reliable framework ensures the reliability and validity of the study. Below is Table 1, showing the results of convergent validity analysis, which ascertains the reliability and validity criteria of the constructs applied in the study. The constructs include Digital Transformation (DT) as the independent variable, Accounting Fraud (AF) as the dependent variable, and Cybersecurity Maturity (CM) as the moderating variable. The table evaluates the constructs based on their range of path coefficient loadings, composite reliability (CR), and average variance extracted (AVE). The results reveal that the Digital Transformation construct, as measured by 11 items, namely DT1-DT11, has a high range of path coefficient loadings, between 0.76 and 0.89. Its internal consistencies, with a composite reliability of 0.91 and an AVE value of 0.70, show that it is highly reliable and accounts for a sufficient amount of variance in its indicators. Therefore, these findings clearly demonstrate the reliability and validity of the digital transformation construct, making it a suitable inclusion in this study.

Table 1: Convergent validity analysis

Constructs	Items	Range of path coefficient loading	CR	AVE
Independent: Digital transformation (DT)	DT1-DT11	0.76-0.89	0.91	0.70
Dependent: Accounting fraud (AF)	AF1- AF8	0.70-0.84	0.89	0.67
Moderator: Cybersecurity maturity (CM)	CM1-CM14	0.72-0.83	0.92	0.74

We measured the AF construct using eight items, specifically AF1-AF8, yielding a path coefficient loading range of 0.70-0.84, as well as a CR of 0.89 and an AVE of 0.67. These results demonstrate the appropriate measurement of the accounting fraud construct within the research framework. The CM construct, measuring 14 items from CM1 to CM14, serves as the moderate variable. The path coefficient loadings range from 0.72 to 0.83, with a CR of 0.92 and an AVE of 0.74. These values demonstrate the robust reliability and validity of the cybersecurity maturity construct, which this study considers a significant moderator in the relationship between digital transformation and accounting fraud.

Table 2 presents the results of the discriminant validity analysis that focuses on three constructs: DT, AF, and CM. Discriminant validity will ensure that the construct is unique and indicates conceptual elements not represented by other constructs in this model. Confirming the robustness of the measurement model and a theoretical framework through this test is crucial. The table below presents the results in a more useful format. The diagonal elements are the square root of AVE for each construct, and the off-diagonal elements represent the correlation between constructs. For AVE to be a discriminant, the square root value for each paired construct must be higher than all the paired values between the constructs shown. This is because the square root value of AVE is higher than the square root value of each construct-correlation relationship (Fornell & Larcker, 1981).

The results reveal that DT's square root of the AVE is 0.837, larger than its estimated correlations with AF and CM of 0.557

and 0.487, respectively. This validates the differentiation of the digital transformation construct from other constructs in this model and its adequate discrimination from them. We also found that AF's square root of AVE was 0.832, higher than its correlation with DT at 0.557 and CM at 0.611. This means that the accounting fraud construct has captured something unique from the study framework and further reinforces its discriminant validity. For CM, the square root of AVE is 0.845, which is higher than its correlations with DT at 0.487 and AF at 0.611. These are confirmations that the cybersecurity maturity construct is also distinct and well-defined within the measurement model. The results of the discriminant validity analysis presented in general provide strong evidence that the constructs are unique and do not suffer from excessive overlap. Each construct therefore represents one theoretical concept and supports the integrity of the measurement model. Fornell and Larcker (1981) recommended thresholds for their findings, indicating their appropriateness for further analysis. Therefore, this analysis ensures the reliability and validity of the overall research framework, presenting the relationships among constructs without any measurement-related confounding. These results provide a sound basis for the subsequent assessment of structural relationships and hypothesis testing in the study.

Table 3 presents the results of statistical testing of the research hypotheses. We derived the path coefficients (B), t-values, and p-values and determined the significance of each hypothesis using the bootstrap method with 5,000 samples. These will help draw further insights on how DT, AF, and CM interlink. The first hypothesis, H_1, was that digital transformation has a negative effect on the accounting fraud risk factor. Therefore, as proposed, the path coefficient shows a negative consequence: B = −0.725, indicating a significant inverse association between digital transformation and accounting fraud. A t-value as high as 12.341, with a P = 0.000 at the 0.001 significant level, supports this. These findings reveal that those organizations that implement the practices of digital transformation effectively reduce the risks of accounting fraud. The result is in line with the previous studies that have pointed out the role of advanced technologies in fraud detection and prevention.

The second hypothesis (H_2) examines the maturity of the cybersecurity protocol and how it moderates the impact of digital transformation on accounting fraud. This interaction term exhibits a positive path coefficient, with B = 0.245, t-value = 4.560, and P = 0.000, indicating a statistically significant moderation effect. This suggests that organizations with high cybersecurity maturity can effectively use digital transformation to reduce their vulnerability to accounting fraud. That is, the organizations that have better cybersecurity will be able to use digital transformation in combating fraud. This means that cybersecurity maturity has a significant role in building organizational resilience against fraud risks. In general, the results of path coefficient analysis provide strong empirical support for the proposed hypotheses. Therefore, we can affirm the support for Hypotheses 1 and 2. This shows how important digital enablers, their changes, and their level of cybersecurity maturity are in fighting modern corporate accounting fraud. The findings contribute to the increasing volume of emerging accounting literature on fraud, which explores aspects of technological advancement and fraud incidents, especially in relation to cybersecurity and its potential for improvement within any agency.

This study tries to find out the effects brought about by digital transformation on the fraud risks in accounting and considers the moderating role of cybersecurity maturity in this relationship. The results provide considerable insights into the dynamics of these constructs and contribute to the understanding of how organizations can exploit digital transformation while protecting themselves from the related risks of fraud. First, H_1 posited that digital transformation would have a significant negative association with the risks of accounting fraud. The strong support at B = −0.725 and P < 0.001 was realized, which agreed with other studies showing the potentiality of digital technologies to improve mechanisms of fraud detection and internal controls. For instance, Putri 2024 and Tiron-Tudor et al. 2022 showed that AI, blockchain, and robotic process automation are among the tools to help an organization enhance operational transparency and identify anomalies that could suggest fraud. This, however, reflects the two-way nature of digital transformation, as suggested by Ghofirin and Algristian (2020) and Luo (2023), who warned that the same digital tools that reduce fraud risks introduce other vulnerabilities fraudsters can capitalize on. Digital transformation significantly lowers the risks of accounting fraud, but these benefits hinge on the careful implementation and management of these technologies.

The second hypothesis, H_2, looked at cybersecurity maturity as a moderator. This was also significant and positive, with B = 0.245 and P < 0.001, showing that the level of maturity of cybersecurity procedures is more important to make sure that digital transformation helps reduce fraud the most. Advanced frameworks in cybersecurity may, as highlighted in prior studies

Table 2: Discriminant validity analysis results

Constructs	Digital transformation (DT)	Accounting fraud (AF)	Cybersecurity maturity (CM)
Digital transformation (DT)	0.837	-	-
Accounting fraud (AF)	0.557	0.832	-
Cybersecurity maturity (CM)	0.487	0.611	0.845

Table 3: Hypotheses results

Path	Hypothesis	B	T-value	P-value	Decision
Digital Transformation -> accounting fraud	H_1	−0.725	12.341	0.000	Accepted
Cybersecurity maturity * digital transformation -> accounting fraud	H_2	0.245	4.560	0.000	Accepted

P<0.001; 2-tailed hypothesis; 5,000 bootstrap samples (e.g., Al-Ghamdi, 2023; Alfaadhel et al., 2023), assist in protecting against the most current and sophisticated forms of fraudulent schemes. Organizations with high cybersecurity practices, including encryption, real-time monitoring, and employee training programs, are better capable of securing their financial systems and reducing any form of vulnerability. Pollini et al. (2021) established that a cybersecurity-conscious culture would ensure greater compliance with security measures and reduce fraud incidents, which the findings also confirm. The findings also add to the literature on the evolving role of emerging technologies in fraud detection and prevention. According to Zhu et al. (2021) and Agboare (2021), technologies like deep learning, forensic accounting tools, and blockchain have revolutionized fraud detection by enabling real-time monitoring and analysis of big datasets in search of fraudulent patterns. This study highlights cybersecurity maturity as the complementary factor that could ensure the functionality of these technologies. The study once again suggests that the security frameworks behind even the most advanced gadgets determine their effectiveness.

The findings of the study are relevant within the context of rapid digital transformation brought about by the COVID-19 pandemic. On one hand, Metwally et al. (2022) claim that increased adoption of digital platforms during the COVID-19 pandemic heightened internal controls and fraud risks. This study follows up on these observations by showing that cybersecurity maturity serves as an important buffer that enables an organization to curtail the risk of fraud, even at a time when technological changes happen so fast, and organizations happen to rely hugely on third-party systems. Fundamentally, the results underline that digital transformation activities are necessary per se but balanced by cybersecurity maturity. After all, these new vulnerabilities are brought along by digitalization-for which the efforts should be supported by a robust and proactive cybersecurity framework-even as digital technologies offer huge opportunities to enhance operational efficiency and fraud detection.

5. CONCLUSION

The study highlights the relationship between digital transformation, the risk of accounting fraud, and cybersecurity maturity. In fact, this study establishes that the risk of accounting fraud goes down considerably with better digital transformation. Among other benefits, digital transformation achieves a better level of operational transparency, simplifies financial reporting procedures, and enhances the effectiveness of fraud detection systems. This, however, is an inverse relationship between digital transformation and fraud risk, highly contingent on the maturity of cybersecurity protocols in an organization. Organizations with well-established cybersecurity measures are in a better position to fully leverage the benefits of digital transformation. This ensures the resilience of both the financial systems and the data involved while protecting the vulnerabilities brought about by digital technologies. The findings of this study have brought into focus the growing need to accompany technological advancement with an inclusive cybersecurity framework that will pave the way toward organizational integrity, protection of sensitive data, and maintenance of stakeholder trust in a greatly complicating and digitalizing business world.

These findings, therefore, provide new information on how digital transformation affects fraud risks and supports the idea that cybersecurity maturity plays a moderating role in reducing cyber fraud incidents. This makes a theoretically and practically useful contribution to preventing fraud in this digital era and fills in some gaps in literature. It also points out that the path ahead requires dual strategies for any organization: investments in state-of-the-art digital technologies while developing appropriate cybersecurity frameworks. An integrated approach, in turn, will further enable an organization to achieve operational efficiency, put in place better fraud prevention measures, and reduce financial and reputational risks. By focusing on innovation and prioritizing security, an organization can effectively mitigate the challenges of the modern digital era. By ensuring the integrity of its financial situation, improving internal controls, and fostering long-term confidence among stakeholders, an organization achieves this.

Despite the study's immense contribution, it has some limitations that future research may resolve. This study only uses data from Jordanian audit and accounting firms, which may limit its applicability to other regions or industries. Future studies may, therefore, extend this research to other countries and different industries to give a wider view of interrelations among digital transformation, cybersecurity maturity, and fraud risks. Moreover, this study used self-reported data; hence, biases may be inevitable. This could potentially lead to participants overstating their organizations' readiness for cybersecurity and their progress toward digital transformation. We might design future research using a mixed-methods approach, combining quantitative data with qualitative interviews to gain a deeper understanding with less potential for bias.

Another possible future research direction might be to investigate other moderating or mediating variables that could affect the relationship between digital transformation and accounting fraud risks. For example, organizational culture, employee digital literacy, leadership commitment to cybersecurity, or regulatory compliance might become important factors in shaping how digital technologies affect fraud prevention. A more detailed analysis of such factors could result in a better and more holistic understanding of the dynamics involved. Longitudinal studies will also be useful in determining how digital transformation, cybersecurity maturity, and fraud risk are related over time. For instance, such studies could explore how continuous improvements in cybersecurity practices influence the long-term effectiveness of digital transformation in mitigating fraud risks. Overcoming some of these limitations and broadening the scope of research would allow further development in understanding how digital transformation affects fraud prevention in the increasingly digital and connected world.

REFERENCES

Abdel-Rahman, M. (2023), Advanced cybersecurity measures in IT service operations and their crucial role in safeguarding enterprise data in a connected world. Eigenpub Review of Science and Technology, 7(1), 138-158.

Aboalganam, K.M., Alzghoul, A. (2025), The impact of digital marketing on the reputation of insurance companies: The role of service quality and brand trust. Insurance Markets and Companies, 16(1), 1-14.

Abousweilem, F., Alzghoul, A., Khaddam, A.A., Khaddam, L.A. (2023), Revealing the effects of business intelligence tools on technostress and withdrawal behavior: The context of a developing country. Information Development, 02666669231207592. https://doi.org/10.1177/02666669231207592

Abu-Dabaseh, F., Alghizzawi, M., Alkhlaifat, B.I., Alzghoul, A., AlSokkar, A.A., Al-Gasawneh, J. (2024), Enhancing Privacy and Security in Decentralized Social Systems: Blockchain-Based Approach. In: 2024 2nd International Conference on Cyber Resilience (ICCR). IEEE. p1-6.

Agboare, E. (2021), Impact of forensic accounting on financial fraud detection in deposit money banks in Nigeria. African Journal of Accounting and Financial Research, 4(3), 74-119.

Al Kasasbeh, O., Khasawneh, O., Alzghoul, A. (2023), The real effects of Fintech on the global financial system. International Journal of Professional Business Review, 8(3), e01425.

Alfaadhel, A., Almomani, I., Ahmed, M. (2023), Risk-based cybersecurity compliance assessment system (rc2as). Applied Sciences, 13(10), 6145.

Al-Ghamdi, B. (2023), Selection of a trustworthy technique for fraud prevention in the digital banking sector. International Journal of Advanced Computer Science and Applications, 14(11), 1124.

Alhanatleh, H., Khaddam, A., Abudabaseh, F., Alghizzawi, M., Alzghoul, A. (2024), Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. Investment Management and Financial Innovations, 21(1), 417.

Alhanatleh, H., Khaddam, A., Alzghoul, A. (2024), Measuring factors affecting consumer attitudes toward metaverse adoption: Islamic banking services setting. Banks and Bank Systems, 19(4), 205-219.

Ali, M.M., Nobi, M.N., Wafik, H.A., Ishmam, M.R., Anika, T.I. (2024), Revealing the accounting problems: An in-depth exploration of accounting challenges and remedies. Global Mainstream Journal of Business, Economics, Development and Project Management, 3(2), 36-44.

AllahRakha, N. (2024), Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. Lex Scientia Law Review, 8(1), 405-432.

Alzghoul, A., Al-Kasasbeh, O. (2024), The moderating role of information technology infrastructure in the relationship between fintech adoption and organizational competitiveness. Investment Management and Financial Innovations, 21(2), 155.

Alzghoul, A., Khaddam, A.A., Alshaar, Q., Irtaimeh, H.J. (2024), Impact of knowledge□oriented leadership on innovative behavior, and employee satisfaction: The mediating role of knowledge□centered culture for sustainable workplace. Business Strategy and Development, 7(1), e304.

Bansal, U., Bharatwal, S., Bagiyam, D.S., Kismawadi, E.R. (2024), Fraud detection in the era of AI: Harnessing technology for a safer digital economy. In: AI-Driven Decentralized Finance and the Future of Finance. United States: IGI Global, p139-160.

Chen, W., Cai, W., Hu, Y., Zhang, Y., Yu, Q. (2024), Gimmick or revolution: Can corporate digital transformation improve accounting information quality? International Journal of Emerging Markets, 19(10), 2966-2990.

Daraojimba, R. (2023), Forensic accounting in the digital age: A U.S. perspective: scrutinizing methods and challenges in digital financial fraud prevention. Finance and Accounting Research Journal, 5(11), 342-360.

Dashkevich, N., Counsell, S., Destefanis, G. (2024), Blockchain financial statements: Innovating financial reporting, accounting, and liquidity management. Future Internet, 16(7), 244.

Ghofirin, M., Algristian, H. (2020), Predicting the rationalization factor that works on accounting fraud at microfinance institution. Kresna Social Science and Humanities Research, 1, 1-9.

Goh, C. (2020), Applying visual analytics to fraud detection using Benford's law. Journal of Corporate Accounting and Finance, 31(4), 202-208.

Ibrahim, U., Eriki, P. (2020), Forensic accounting and incidence of fraud detection. International Journal of Finance and Banking Studies, 9(2), 72-81.

Imjai, N., Promma, W., Visedsun, N., Usman, B., Aujirapongpan, S. (2025), Fraud detection skills of Thai Gen Z accountants: The roles of digital competency, data science literacy and diagnostic skills. International Journal of Information Management Data Insights, 5(1), 100308.

Karaki, B.A., Al-Kasasbeh, O., Alassuli, A., Alzghoul, A. (2023), The impact of the digital economy on carbon emissions using the STIRPAT model. International Journal of Energy Economics and Policy, 13(5), 139-143.

Luo, Y. (2023), Reduce fraud: From fraud motivation to fraud avoidance. Advances in Economics Management and Political Sciences, 9(1), 174-179.

Metwally, A.B., Abdelazim, S.I., Almarji, M.T. (2022), Internal auditors' role in confronting cyber and fraud risks related to outsourcing insurance: An exploratory study. Alexandria Journal of Accounting Research, 6(3), 1-31.

Odeyemi, O., Ibeh, C.V., Mhlongo, N.Z., Asuzu, O.F., Awonuga, K.F., Olatoye, F.O. (2024), Forensic accounting and fraud detection: A review of techniques in the digital age. Finance and Accounting Research Journal, 6(2), 202-214.

Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F.,… & Guerri, D. (2021), Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition Technology and Work, 24(2), 371-390.

Putnoki, A.M., Orosz, T. (2023), Artificial Intelligence and Cognitive Information Systems: Revolutionizing Business with Generative Artificial Intelligence and Robotic Process Automation. In: The International Conference on Recent Innovations in Computing. Singapore: Springer Nature Singapore. p39-70.

Putri, M. (2024), Analysis of factors and fraud preventive efforts in company financial reports: A literature review study. Asia Pacific Fraud Journal, 9(1), 107-118.

Ridzuan, N., Said, J., Razali, F., Manan, D., Sulaiman, N. (2022), Examining the role of personality traits, digital technology skills and competency on the effectiveness of fraud risk assessment among external auditors. Journal of Risk and Financial Management, 15(11), 536.

Roszkowska, P. (2021), Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. Journal of Accounting and Organizational Change, 17(2), 164-196.

Salah, A.H., Alzghoul, A. (2024), Assessing the moderating role of customer orientation on the impact of business intelligence tools on digital marketing strategy optimization. International Review of Management and Marketing, 14(3), 18-25.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M.A., Muhammad, Z. (2024), A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. International Cybersecurity Law Review, 5, 533-561.

Suela, L.C. (2024), Online fraud exposed: tactics and strategies of cyber scammers. International Journal of Scientific Research in Engineering and Management, 8(4), 1-5.

Suri, V.K. (2022), Functional Automation and Digital Transformation. United States: Dorrance Publishing.

Tam, K., & Jones, K. (2019), MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18, 129-163.

Tariq, T., Javaid, F., Syed, R., Zubair, M., Fayyaz, B. (2022), Challenges in security and privacy posed by blockchain technology. Journal of Independent Studies and Research-Computing, 20(2), 1-9.

Tiron-Tudor, A., Donțu, A., Bresfelean, V. (2022), Emerging technologies' contribution to the digital transformation in accountancy firms. Electronics, 11(22), 3818.

Vance, D., Jin, M., Price, C., Nimbalkar, S., Wenning, T. (2023), Smart manufacturing maturity models and their applicability: A review. Journal of Manufacturing Technology Management, 34(5), 735-770.

Zhang, Y., Xiong, F., Xie, Y., Fan, X., Gu, H. (2020), The impact of artificial intelligence and blockchain on the accounting profession. IEEE Access, 8, 110461-110477.

Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q.,… & Li, J. (2021), Intelligent financial fraud detection practices in post-pandemic era. The Innovation, 2(4), 100176.