www.refaad.com

Global Journal of Economics and Business (GJEB)

المجلة العالمية للاقتصاد والأعمال

Journal Homepage: https://www.refaad.com/Journal/Index/2

E-ISSN 2519-9293 | P-ISSN 2519-9285

Vol. 16, Issue 5, 2026, pp. 629 - 638



The Impact of Internal Control Systems on Minimizing Fraud: The Case of the Banking Sector in Saudi Arabia

Rasha Abdulrhman Fallatah[1*]

[1] Collage of Business Administration, Accounting Department, Taif University, KSA.

[*] Corresponding Author: Rasha Fallatah (rasha@tu.edu.sa)

أثر نظم الرقابة الداخلية في الحد من الاحتيال: دراسة حالة القطاع المصرفي في المملكة العربية السعودية

رشا عبد الرحمن فلاتة[1*]

[1] كلية إدارة الأعمال- قسم المحاسبة- جامعة الطائف- المملكة العربية السعودية.

*الباحث المراسل: رشا فلاتة (rasha@tu.edu.sa)

This file is licensed under a *Creative Commons Attribution 4.0 International*

Received استلام البحث	Revised مراجعة البحث	Accepted قبول البحث
2026/2/23	2026/5/24	2026/6/2

DOI: https://doi.org/10.31559/GJEB2026.16.5.7

Abstract:

Objectives: This study examines the impact of internal control systems on fraud prevention in Saudi Arabia's banking sector, with particular emphasis on the five COSO internal control components and the mediating role of cybersecurity integration.

Methods: The study adopted a quantitative explanatory research design. Data were collected through a structured questionnaire distributed to employees working in risk management, compliance, internal auditing, and IT security functions in Saudi commercial banks. A total of 312 valid responses were analyzed using SPSS 28.0 and SmartPLS Descriptive statistics, correlation analysis, multiple regression analysis, and structural equation modeling (SEM) were employed to test the proposed hypotheses.

Results: The findings reveal that all internal control components have statistically significant positive effects on fraud prevention within Saudi banks. Risk assessment, control activities, and monitoring activities demonstrate the strongest predictive effects in minimizing fraudulent activities. The results also show a partial mediating effect of cybersecurity integration, indicating that digital monitoring systems and cybersecurity practices enhance the effectiveness of traditional internal control mechanisms in reducing fraud risk.

Conclusions: The study concludes that effective internal control systems play a critical role in strengthening fraud prevention practices in the Saudi banking sector. The findings offer practical implications for bank management, internal auditors, compliance officers, and regulatory authorities, including the Saudi Central Bank (SAMA), by supporting improved governance practices, stronger internal controls, and reduced fraud risks within Saudi banks.

Keywords: *Internal Control Systems; Fraud Prevention; Saudi Banking Sector; Risk Assessment; Corporate Governance; Cybersecurity; SAMA.*

الملخص:

الأهداف: هدفت هذه الدراسة إلى فحص أثر نظم الرقابة الداخلية في الحد من الاحتيال في القطاع المصرفي بالمملكة العربية السعودية، في ظل التوسع المتسارع في الخدمات المصرفية الرقمية وتزايد مخاطر الاحتيال المالي والجرائم السيبرانية. وركزت الدراسة على مكونات إطار COSO الخمسة، وهي: بيئة الرقابة، وتقييم المخاطر، والأنشطة الرقابية، والمعلومات والاتصال، وأنشطة المتابعة، إضافة إلى دراسة الدور الوسيط للتكامل السيبراني في تعزيز فعالية مكافحة الاحتيال داخل البنوك السعودية.

المنهجية: اعتمدت الدراسة على المنهج الكمي التفسيري، وتم جمع البيانات من خلال استبانة وُزعت على العاملين في مجالات المراجعة الداخلية، وإدارة المخاطر، والالتزام، والأمن السيبراني في البنوك التجارية السعودية. وبلغ عدد الاستبانات الصالحة للتحليل 312 استبانة. كما تم تحليل البيانات باستخدام برنامجي SPSS 28.0 و SmartPLS 4، وذلك بالاعتماد على الإحصاء الوصفي، وتحليل الارتباط، والانحدار المتعدد، وتحليل المسار لاختبار فرضيات الدراسة.

النتائج: أظهرت نتائج الدراسة وجود أثر إيجابي ذي دلالة إحصائية لجميع مكونات نظم الرقابة الداخلية في الحد من الاحتيال في القطاع المصرفي السعودي. كما تبين أن تقييم المخاطر، والأنشطة الرقابية، وأنشطة المتابعة تمثل أكثر العوامل تأثيرًا في تعزيز فعالية مكافحة الاحتيال داخل البنوك السعودية. كذلك كشفت النتائج عن وجود أثر وساطة جزئي للتكامل السيبراني، مما يشير إلى أن دمج أدوات الأمن السيبراني وأنظمة المراقبة الرقمية مع نظم الرقابة الداخلية التقليدية يسهم في تحسين قدرة البنوك على اكتشاف الممارسات الاحتيالية وتقليل مخاطرها.

الخلاصة: خلصت الدراسة إلى أن نظم الرقابة الداخلية الفعالة تؤدي دورًا جوهريًا في تعزيز ممارسات مكافحة الاحتيال وتحسين الحوكمة داخل القطاع المصرفي السعودي. كما تقدم الدراسة دلالات عملية مهمة للإدارة المصرفية، والمراجعين الداخليين، والجهات الرقابية، وفي مقدمتها البنك المركزي السعودي (SAMA)، بما يسهم في دعم فعالية الرقابة الداخلية، وتعزيز الشفافية، وتقليل مخاطر الاحتيال داخل البنوك السعودية.

الكلمات المفتاحية: *نظم الرقابة الداخلية؛ الاحتيال المالي؛ القطاع المصرفي السعودي؛ مكافحة الاحتيال؛ إدارة المخاطر؛ الأمن السيبراني؛ الحوكمة المصرفية.*

Citation

Fallatah, R. A. (2026). The Impact of Internal Control Systems on Minimizing Fraud: The Case of the Banking Sector in Saudi Arabia . *Global Journal of Economics and Business*, 16(5), 629-638. https://doi.org/10.31559/GJEB2026.16.5.7

1 Introduction

Fraud in the banking industry remains one of the most serious challenges facing financial institutions worldwide. Beyond financial losses, fraudulent activities can damage investor confidence, weaken financial stability, and reduce public trust in banking systems. The rapid growth of digital banking, electronic payment platforms, and financial technology has further increased exposure to sophisticated financial and cyber fraud. As a result, strengthening internal control systems has become a strategic priority for banks and regulatory authorities alike (Oduro et al., 2025).

In Saudi Arabia, the banking sector plays a central role in supporting the objectives of Vision 2030 and promoting sustainable economic growth. Vision 2030 emphasizes economic diversification, technological innovation, and digital development across key sectors, including financial services (U.S. International Trade Administration, 2025). In response to these developments, Saudi banks operate within a comprehensive regulatory environment supervised by the Saudi Central Bank (SAMA), which has introduced governance, compliance, anti-fraud, and cybersecurity regulations aimed at improving transparency and institutional accountability. Nevertheless, fraud risks continue to evolve alongside the increasing complexity of banking operations and digital financial services.

Internal control systems are widely viewed as essential mechanisms for reducing fraud risk and improving organizational governance. Based on the COSO framework, internal controls consist of five integrated components: control environment, risk assessment, control activities, information and communication, and monitoring activities. Together, these components help organizations safeguard assets, ensure reliable financial reporting, support regulatory compliance, and reduce opportunities for fraudulent behavior (Harber & Marx, 2020).

The ongoing expansion of digital banking technologies in Saudi Arabia has also transformed fraud detection and prevention practices. Banks increasingly rely on artificial intelligence, automated monitoring systems, biometric verification, and real-time analytics to strengthen internal controls and improve fraud detection capabilities. Government initiatives supporting artificial intelligence and digital infrastructure have accelerated the modernization of banking services and digital payment systems across the Kingdom (U.S. International Trade Administration, 2025). However, the effectiveness of these technologies largely depends on the quality of the underlying internal control framework. Weak monitoring procedures, poor communication channels, and inadequate segregation of duties may still create opportunities for fraud, even within technologically advanced banking environments.

Recognizing the importance of strong governance and risk management, SAMA has established regulatory guidelines that emphasize effective internal control practices within Saudi banks. These guidelines require boards of directors and senior management to review risk management strategies regularly and ensure the implementation of appropriate control procedures for identifying, monitoring, and managing financial risks (International Monetary Fund, 2013). In addition, supervisory inspections are conducted to evaluate the adequacy of banks' monitoring systems, credit administration procedures, and internal control practices (International Monetary Fund, 2013). Such regulatory oversight highlights the importance of internal controls in protecting financial institutions from fraudulent activities.

Although prior studies have examined fraud prevention and internal control systems in different international contexts, empirical evidence relating specifically to the Saudi banking sector remains limited. Existing research has largely focused on identifying relationships between variables rather than examining the actual impact of internal control components on fraud minimization. Moreover, the rapid expansion of digital banking services has created new operational and cybersecurity challenges that require further investigation.

Accordingly, this study examines the impact of internal control systems on minimizing fraud in the Saudi banking sector by evaluating the effects of the five COSO internal control components on fraud prevention practices. The study also explores the role of cybersecurity integration in enhancing the effectiveness of internal controls within Saudi banks. Using a quantitative explanatory research design and regression-based analysis, this study contributes to the growing literature on banking governance, fraud prevention, and internal control effectiveness in emerging economies.

The findings of this study are expected to provide practical implications for bank managers, internal auditors, compliance officers, policymakers, and regulatory authorities such as SAMA. In addition, the study supports the objectives of Vision 2030 by promoting stronger governance practices, greater transparency, and sustainable development within the Saudi banking sector.

2 Literature Review

Previous literature has consistently emphasized the importance of internal control systems in reducing fraud and improving organizational governance. Earlier studies mainly focused on the role of institutional capabilities, audit procedures, and governance structures in strengthening fraud prevention mechanisms. For example, Popoola et al. (2016) examined the moderating role of institutional capability in enhancing the effectiveness of internal control systems within financial institutions. Their findings indicated that strong institutional support improves organizations' ability to detect and reduce fraudulent activities.

Meiryani et al. (2019) highlighted internal control systems as fundamental mechanisms for fraud prevention and organizational accountability. Similarly, Harber and Marx (2020) explained the significance of the five COSO internal control components - control environment, risk assessment, control activities, information and communication, and monitoring - in establishing an effective fraud prevention framework.

From 2021 onward, research increasingly focused on the effectiveness of internal auditing, governance practices, and digital transformation in minimizing fraud risks. Agustina et al. (2021) found that auditors' professional skepticism significantly improves fraud detection capabilities. During the same period, Hay et al. (2021) examined the resilience of internal control systems during the COVID-19 pandemic and concluded that adaptable control mechanisms are essential for maintaining effective fraud prevention under crisis conditions. In the Saudi context, Al-Harbi and Al-Ahmari (2021) reported that higher internal audit quality positively contributes to fraud prevention within Saudi commercial banks.

In 2022, the literature expanded to include governance, corruption risk, and technology-driven fraud prevention mechanisms. Pizzi et al. (2021) and Grayston (2022) emphasized the growing importance of digital auditing tools and data analytics in improving fraud detection processes. Alberti et al. (2022) examined the influence of audit firm culture on internal control effectiveness, while Fung et al. (2022) demonstrated how corruption culture may weaken internal audit quality and organizational controls. Rashid et al. (2022) also developed a comparative framework for evaluating fraud prevention strategies in developed and developing countries. Within Saudi Arabia, the Institute of Internal Auditors Saudi Arabia (2022) stressed the importance of compliance with SAMA regulations in strengthening fraud prevention practices across financial institutions.

More recent studies have shifted attention toward cybersecurity, digital banking risks, and artificial intelligence applications in fraud detection. Alqassem (2022) analyzed the effectiveness of SAMA compliance regulations in improving internal audit effectiveness and reducing fraud risk in Saudi banks. Pilonato (2022) discussed the role of accounting systems in either facilitating or limiting corruption networks, whereas Sulaiman et al. (2022) examined how audit rotation and governance mechanisms contribute to improving internal control effectiveness.

Research published in 2023 further highlighted the growing integration between internal controls and digital technologies. Alzeban (2023) examined the mediating role of organizational ethics in the relationship between internal controls and fraud prevention within Saudi institutions. Similarly, Al-Shammari et al. (2023) found that implementing COSO-based internal control frameworks significantly reduces fraudulent activities in Saudi commercial banks. Baz et al. (2023) argued that weak internal controls and insufficient fraud awareness may negatively affect the financial stability of Saudi banks. In addition, Kumar and Yadav (2023) warned that the rapid growth of online banking services increases exposure to cyber fraud risks, while Aburaya and Barnat (2023) emphasized the importance of legal and regulatory measures in combating identity-based banking fraud in Saudi Arabia.

The most recent studies published between 2024 and 2025 have concentrated on digital transformation, artificial intelligence, and cybersecurity integration within banking systems. Alsulami and Almutairi (2024) investigated the digital transformation of internal control systems in the Saudi banking sector and highlighted the importance of technological integration in enhancing fraud monitoring practices. Waliullah et al. (2025) demonstrated that advanced technologies, such as blockchain and biometric authentication, significantly reduce opportunities for fraud in digital banking environments. Likewise, Chen et al. (2025) concluded that artificial intelligence-based fraud detection models are highly effective in identifying anomalies and suspicious transactions in real time.

Although previous studies provide valuable insights into internal controls and fraud prevention, several research gaps remain. First, many earlier studies focused primarily on identifying relationships between variables rather than examining the predictive impact of internal control components on fraud minimization. Second, limited empirical evidence exists regarding the Saudi banking sector, particularly under the current environment of rapid digital transformation and increasing cybersecurity threats. Third, prior studies often

examined internal controls, governance, cybersecurity, or fraud prevention separately, without integrating these dimensions into a unified analytical framework.

Accordingly, the current study contributes to the literature by examining the impact of the five COSO internal control components on fraud minimization within Saudi banks using an explanatory quantitative approach. Unlike many prior studies, this research also incorporates cybersecurity integration as a mediating factor to better reflect the evolving digital banking environment in Saudi Arabia. In doing so, the study provides a more comprehensive understanding of how traditional internal control systems and modern technological tools collectively contribute to fraud prevention within the Saudi banking sector.

3 Theoretical Framework

This study is underpinned by two complementary organizational theories that provide a conceptual lens for understanding the effectiveness of internal control systems in fraud prevention within financial institutions: Contingency Theory and Agency Theory.

Contingency Theory posits that there is no universally optimal structure or system of control; rather, the design and effectiveness of internal controls depend on the specific context in which an organization operates. Key organizational variables, such as size, structure, technological sophistication, and environmental pressures, significantly influence the nature and performance of internal control mechanisms. Within the Saudi banking context, such variables include regulatory compliance requirements, including guidelines issued by SAMA, levels of digitization, the complexity of financial products, and degrees of operational risk. Consequently, banks must tailor their internal control frameworks to align with these contextual demands in order to mitigate fraud risk effectively. This theory supports the view that internal controls are not static or uniform but must evolve to suit each bank's internal dynamics and external environment (Donaldson, 2001; Otley, 1980).

In parallel, Agency Theory provides further theoretical grounding by addressing the inherent conflict of interest that arises in principal-agent relationships, particularly between shareholders and bank executives. The theory asserts that agents may not always act in the best interests of principals unless appropriate monitoring and control mechanisms are in place. Internal controls serve as these mechanisms by establishing checks and balances, such as segregation of duties, formal approval hierarchies, internal audit functions, compliance monitoring, and oversight committees. In the Saudi banking sector, the implementation of these controls plays a vital role in curbing opportunistic behavior by aligning managerial actions with stakeholder objectives and reinforcing institutional integrity (Jensen & Meckling, 1976; Eisenhardt, 1989).

Together, these two theoretical perspectives provide a comprehensive explanation of how internal control systems contribute to fraud prevention. Contingency Theory highlights the importance of contextual alignment in the design of control mechanisms, while Agency Theory underscores their necessity for mitigating agency problems and promoting ethical behavior. Applied to this study, the integration of both theories strengthens the argument that effective, well-structured, and context-sensitive internal control systems are essential for reducing fraud within Saudi banks.

4 Research Hypotheses

Based on the literature review and the theoretical framework underpinning this study, the following hypotheses were developed to examine the impact of internal control system components on fraud prevention in the Saudi banking sector:

- H1: The control environment has a significant positive impact on fraud prevention in Saudi banks.
- H2: Risk assessment practices have a significant positive impact on fraud prevention in Saudi banks.
- H3: Control activities have a significant positive impact on fraud prevention in Saudi banks.
- H4: Information and communication systems have a significant positive impact on fraud prevention in Saudi banks.
- H5: Monitoring mechanisms have a significant positive impact on fraud prevention in Saudi banks.

These hypotheses were tested using empirical data collected from professionals working in risk management, compliance, internal auditing, and related control functions within Saudi banks. The study employed regression analysis and structural equation modeling techniques to examine the predictive effects of internal control components on fraud prevention outcomes.

5 Methodology

5.1 Research Design

This study adopted a quantitative explanatory research design. A structured questionnaire was developed to measure the impact of internal control components on fraud prevention within Saudi commercial banks.

5.2 Population and Sample

The target population consisted of employees working in Saudi commercial banks, particularly professionals involved in risk management, compliance, internal auditing, and IT security functions. A purposive sampling technique was used to ensure that respondents possessed sufficient knowledge and practical experience related to internal control systems and fraud prevention practices within the banking sector.

A total of 400 questionnaires were distributed across 10 Saudi commercial banks. Of these, 327 responses were received. After incomplete questionnaires were excluded, 312 valid responses were retained for statistical analysis, representing a response rate of 78%. The selected sample was considered appropriate because the respondents were directly involved in control, compliance, auditing, and risk management activities within their respective institutions.

5.3 Data Collection Instrument

Data were collected using a structured questionnaire developed based on the COSO internal control framework and prior studies related to fraud prevention and banking governance. The questionnaire was divided into four sections.

The first section collected demographic information about the respondents, including professional position, years of experience, and educational background. The second section measured the five components of internal control systems, namely control environment, risk assessment, control activities, information and communication, and monitoring activities, using 20 measurement items. The third section focused on cybersecurity and digital control practices within Saudi banks and included eight items. The final section measured fraud prevention effectiveness using six indicators related to fraud detection, monitoring efficiency, and risk reduction.

All items were measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree).

5.4 Validity and Reliability

Content and face validity were verified through expert review. A pilot test (n = 50) showed high internal consistency, with Cronbach's alpha values ranging from 0.85 to 0.89 across the different sections.

5.5 Data Analysis Techniques

Descriptive statistics, Pearson correlation, and multiple regression analysis were performed using SPSS 28.0. In addition, SmartPLS 4 was used for path analysis to examine the structural relationships between variables. Mediation analysis was conducted to explore the potential role of cybersecurity integration in enhancing internal control effectiveness.

6 Results and Analysis

The collected data were analyzed using SPSS 28.0 and SmartPLS 4 to examine the impact of internal control systems on fraud prevention in the Saudi banking sector. The analysis included descriptive statistics, correlation analysis, multiple regression analysis, and mediation testing. The findings revealed several important results regarding the effectiveness of internal control components in minimizing fraudulent activities within Saudi banks.

6.1 Descriptive Statistics

Descriptive statistical analysis was conducted to examine respondents' characteristics and evaluate perceptions regarding internal control systems and fraud prevention practices within Saudi banks. The respondents represented different professional roles, including internal auditors, compliance officers, risk managers, and IT security specialists. Most participants had more than five years of professional experience in banking and financial control functions, indicating that the respondents possessed sufficient professional knowledge relevant to the study variables.

The findings showed that the mean scores for all five internal control dimensions exceeded 3.8, indicating a relatively high level of implementation of internal control practices across the surveyed banks. Fraud prevention indicators recorded an average mean score of 4.1, suggesting that Saudi banks place considerable emphasis on fraud prevention and monitoring activities. Among the five dimensions, risk assessment and monitoring activities achieved the highest mean scores, reflecting the increasing attention given to fraud risk identification and supervisory procedures within the Saudi banking sector.

Table 1: Descriptive Statistics of Study Variables

Variable	Mean	Std. Deviation
Control Environment	3.89	0.64
Risk Assessment	4.12	0.58
Control Activities	3.97	0.61
Information and Communication	3.85	0.66
Monitoring Activities	4.08	0.57
Fraud Prevention	4.10	0.55

The descriptive statistics indicate that all study variables recorded relatively high mean scores, suggesting strong implementation of internal control practices and fraud prevention measures within Saudi banks.

6.2 Preliminary Correlation Analysis

Pearson correlation analysis was conducted as a preliminary procedure to examine the direction and strength of associations between internal control components and fraud prevention before performing regression analysis.

The results revealed positive and statistically significant associations between all internal control dimensions and fraud prevention outcomes. Risk assessment showed the strongest correlation with fraud prevention ($r = 0.65$, $p < 0.01$), followed by monitoring activities ($r = 0.64$, $p < 0.01$), control activities ($r = 0.61$, $p < 0.01$), control environment ($r = 0.59$, $p < 0.01$), and information and communication systems ($r = 0.56$, $p < 0.01$).

These findings indicate that stronger internal control practices are associated with improved fraud prevention within Saudi banks. However, the primary focus of the study was to examine the predictive impact of internal control components through regression and structural equation modeling analysis.

Table 2: Correlation Analysis

Variables	1	2	3	4	5	6
1. Control Environment	1					
2. Risk Assessment	0.54**	1				
3. Control Activities	0.49**	0.61**	1			
4. Information and Communication	0.46**	0.53**	0.57**	1		
5. Monitoring Activities	0.51**	0.64**	0.59**	0.55**	1	
6. Fraud Prevention	0.59**	0.65**	0.61**	0.56**	0.64**	1

Note: ** p < 0.01.

The regression results indicate that all internal control dimensions have statistically significant positive effects on fraud prevention. Risk assessment demonstrated the strongest predictive effect, followed by control activities and monitoring activities. Accordingly, all study hypotheses were supported.

6.3 Regression Analysis and Hypotheses Testing

Multiple regression analysis was employed to test the study hypotheses and examine the impact of internal control system components on fraud prevention. The regression model produced an R^2 value of 0.47, indicating that approximately 47% of the variance in fraud prevention outcomes was explained by the five internal control dimensions included in the model.

The results demonstrated that all internal control components had statistically significant positive effects on fraud prevention. Risk assessment recorded the strongest predictive effect on fraud prevention ($\beta = 0.32$, $p < 0.001$), followed by control activities ($\beta = 0.26$, $p < 0.01$) and monitoring activities ($\beta = 0.21$, $p < 0.01$). In addition, the control environment ($\beta = 0.18$, $p < 0.05$) and information and communication systems ($\beta = 0.17$, $p < 0.05$) also showed significant positive effects on fraud prevention outcomes.

Based on these findings, all five hypotheses were accepted. The results confirm that effective internal control systems contribute significantly to minimizing fraudulent activities within the Saudi banking sector.

Table 3: Regression Results and Hypotheses Testing

Hypothesis	β	t-value	p-value	Decision
H1: Control Environment → Fraud Prevention	0.18	2.41	< 0.05	Supported
H2: Risk Assessment → Fraud Prevention	0.32	4.88	< 0.001	Supported
H3: Control Activities → Fraud Prevention	0.26	3.76	< 0.01	Supported
H4: Information and Communication → Fraud Prevention	0.17	2.19	< 0.05	Supported
H5: Monitoring → Fraud Prevention	0.21	3.12	< 0.01	Supported

6.4 Mediation Effect of Cybersecurity Integration

Structural equation modeling (SEM) using SmartPLS 4 was conducted to examine the mediating effect of cybersecurity integration on the relationship between internal control systems and fraud prevention.

Table 4: Mediation Analysis Results

Relationship	Direct Effect	Indirect Effect	Mediation Type
Internal Controls → Fraud Prevention	0.58	0.14	Partial Mediation

The mediation analysis revealed that cybersecurity integration partially strengthens the relationship between internal control systems and fraud prevention within Saudi banks. In particular, digital monitoring systems, automated reporting tools, and real-time fraud detection technologies contributed to improving the effectiveness of internal control practices. These findings highlight the importance of combining traditional internal control procedures with advanced cybersecurity mechanisms to reduce fraud risk and enhance governance practices in the Saudi banking sector.

7 Discussion

The findings of this study reaffirm the critical role of internal control systems in strengthening fraud prevention practices within the Saudi banking sector. The results revealed statistically significant positive effects for all five COSO internal control components on fraud prevention outcomes, supporting both Contingency Theory and Agency Theory. These findings suggest that effective internal control systems contribute substantially to improving governance practices, enhancing organizational accountability, and reducing opportunities for fraudulent activities within Saudi banks.

Among the examined components, risk assessment emerged as the most influential factor affecting fraud prevention effectiveness. This finding highlights the importance of continuously identifying, evaluating, and prioritizing potential risks in order to minimize fraudulent activities within banking institutions. Saudi banks that actively assess operational, financial, and cybersecurity risks are better positioned to implement appropriate preventive and corrective control measures, particularly within a rapidly evolving digital banking environment and under the regulatory oversight of SAMA.

The findings further indicated that control activities and monitoring mechanisms have strong predictive effects on fraud prevention. Control activities such as segregation of duties, authorization procedures, reconciliations, and audit trails help reduce operational weaknesses and limit opportunities for fraudulent behavior. Similarly, monitoring activities strengthen supervisory oversight and improve the early detection of irregular transactions and suspicious activities. These mechanisms reflect management's ongoing commitment to maintaining effective internal control systems and promoting a culture of transparency and accountability within Saudi banks.

Although information and communication systems demonstrated the weakest predictive effect among the examined variables, the relationship remained statistically significant. This finding may indicate the need for stronger communication channels, enhanced fraud awareness programs, and more effective coordination among the departments responsible for compliance, risk management, and fraud detection within banking institutions.

The mediation analysis also revealed that cybersecurity integration partially strengthens the relationship between internal control systems and fraud prevention. The increasing adoption of automated alerts, real-time analytics, biometric authentication, and digital monitoring systems has improved the ability of Saudi banks to detect and prevent fraudulent activities more efficiently. These findings suggest that integrating cybersecurity practices with traditional internal control procedures has become increasingly important in strengthening fraud prevention capabilities within modern banking environments.

Overall, the findings are consistent with prior international and regional studies emphasizing the importance of internal control effectiveness, governance practices, and digital transformation in reducing fraud risk within financial institutions. The results also provide empirical support for SAMA's ongoing efforts to strengthen governance, compliance, cybersecurity, and risk management practices across the Saudi banking sector in line with the objectives of Vision 2030.

7.1 Recommendations

- Enhance risk assessment frameworks by establishing dynamic risk registers supported by fraud analytics and real-time monitoring systems.
- Invest in cybersecurity by integrating internal controls with AI-based fraud detection tools and secure data platforms.
- Strengthen monitoring activities by creating independent audit and fraud risk teams with clear escalation procedures.
- Foster an ethical culture by promoting regular staff training on ethics and fraud detection and by implementing anonymous whistleblowing mechanisms.
- Standardize internal control practices across banks by encouraging SAMA to mandate baseline internal control requirements and benchmarks.

8 Conclusion

The research demonstrates that internal control systems, especially risk assessment, monitoring, and control activities, play a vital role in minimizing fraud within the Saudi banking sector. Through empirical analysis, the study confirms that banks with robust internal control frameworks experience lower fraud exposure.

As the industry continues to digitize, a hybrid approach that combines strong traditional controls with emerging technologies is essential. Institutions and regulators must work together to maintain a proactive fraud prevention environment. Future research should explore the longitudinal impacts of regulatory interventions and examine the role of corporate culture and leadership in enhancing internal controls.

8.1 Limitations

While this study contributes valuable insights, it is subject to several limitations. First, it focuses solely on commercial banks and excludes other financial institutions such as Islamic banks, fintech firms, and insurance entities. Second, the data are self-reported and may therefore carry inherent bias. Finally, the cross-sectional design limits the ability to assess long-term changes. Future studies should consider qualitative interviews and longitudinal data to enrich the findings.

References

Aburaya, R., & Barnat, N. (2023). Legal frameworks for combating cyber fraud in Saudi Arabia. *Migration Letters,* 20(4), 115-130.

Agustina, F., Nurkholis, N., & Rusydi, M. (2021). Auditors' professional skepticism and fraud detection. International *Journal of Research in Business and Social Science,* 10(4), 275-287.

Al-Busaidi, K., & Olfman, L. (2021). Business continuity and internal controls in Gulf banks. *International Journal of Accounting Information Systems,* 42, 100541.

Al-Harbi, S., & Al-Ahmari, R. (2021). Internal audit quality and fraud prevention in Saudi commercial banks. *Saudi Journal of Accounting and Finance,* 5(3), 45-62.

Al-Shammari, A., Al-Qahtani, M., & Khan, N. (2023). COSO-based internal control effectiveness in Saudi banks. *Journal of Islamic Banking Studies,* 4(1), 91-110.

Alabdullah, T. T. Y., et al. (2023). Audit committee and fraud prevention. *Journal of Governance and Integrity,* 6(1), 12-24.

Alberti, C. T., Bedard, J. C., Bik, O., & Vanstraelen, A. (2022). Audit firm culture: Recent developments and trends in the literature. *European Accounting Review,* 31(1), 59-109. [DOI]

Alnasser, S. A., & Al-Saleh, N. (2021). Corporate governance in Saudi banks. *International Journal of Economics and Financial Issues,* 11(2), 72-80.

Alqassem, H. (2022). SAMA compliance and its impact on internal audit effectiveness in fraud mitigation. *Arabian Journal of Auditing Research,* 6(2), 121-137.

Alsulami, A., & Almutairi, H. (2024). Digital transformation of internal controls in the Saudi banking sector. *Journal of Financial Technology and Compliance,* 8(1), 33-50.

Alzahrani, S., & Alghamdi, S. (2022). Fraud risk perception in Saudi Arabia. *Middle East Journal of Business,* 17(3), 23-31.

Alzeban, A. (2023). Ethical culture and internal control systems in Saudi Arabia. *Middle East Journal of Governance,* 7(2), 54-72.

Ameen, A., et al. (2021). AIS impact on fraud detection in the Gulf. *International Journal of Accounting and Financial Reporting Management Sciences,* 11(3), 68-80.

Ananzeh, I. E. N. (2022). Audit quality and fraud prevention in Arab banks. *International Journal of Financial Studies,* 10(1), 31.

Atieh, A. M., & Al-Tahat, M. D. (2021). Risk management and internal audit. *Accounting and Finance Research,* 10(4), 108-116.

Bakri, H. H. M., & Mohamed, N. (2022). E-governance and fraud prevention. *Journal of Information Systems and Computing Research,* 5(2), 79-91.

Baz, R., AlSuwailem, N., & Mahfouz, Y. (2023). The role of internal control and information sharing in preventing fraud in Saudi banks. ResearchGate Preprint.

Bwerinofa Petrozzello, C. (2023). Preventing fraud with internal controls: A refresher. *Journal of Accountancy.* https://www.journalofaccountancy.com/issues/2023/aug/preventing-fraud-with-internal-controls-a-refresher.html

Chen, J., Zhang, H., & Liu, Y. (2025). A systematic review on deep learning models for financial fraud detection. arXiv Preprint, arXiv:2502.00201.

Darweesh, D., & Al-Ghamdi, S. (2022). Blockchain in Saudi reporting. *Journal of Emerging Technologies in Accounting,* 19(2), 147-166.

Donaldson, L. (2001). *The contingency theory of organizations*. SAGE Publications.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of Management Review, 14(1), 57-74. [DOI]

Fung, S., Pham, V. T., & Raman, K. K. (2022). Client corruption culture and audit quality. *Review of Quantitative Finance and Accounting,* 59(3), 1133-1171. [DOI]

Grayston, C. (2022). Audit down but not out. *International Journal of Auditing,* 26(1), 8-11. [DOI]

Hamdan, A. M., & Mushtaha, S. (2023). Audit committee independence in Saudi firms. *Corporate Ownership and Control,* 20(3), 85-98.

Harber, M., & Marx, B. (2020). Auditor independence and professional scepticism in South Africa. *South African Journal of Economic and Management Sciences,* 23(1), 1-12. [DOI]

Hay, D., Shires, K., & Van Dyk, D. (2021). Auditing in the time of COVID. *Pacific Accounting Review,* 33(2), 179-188.

Institute of Internal Auditors Saudi Arabia. (2022). *Annual report on internal control compliance*.

International Monetary Fund. (2013). *Saudi Arabia: Financial sector assessment program update - Detailed assessment of observance of the Basel core principles for effective banking supervision* (IMF Country Report No. 13/213).

Jaber, R., & Al-Esmail, R. (2024). Whistleblowing in GCC banks. Ethics & Behavior, 34(1), 112-129.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305-360. [DOI]

Khattab, K. O., & Hammad, L. (2023). AI-driven audit analytics in Saudi Arabia. *AI and Society,* 39(2), 301-316.

Kumar, R., & Yadav, V. (2023). *Fraud and compliance guide for Saudi fintechs*. LinkedIn Insights. https://www.linkedin.com/pulse/fraud-compliance-guide-saudi-fintechs-trustdecision-gujdc

Meiryani, M., Fitriani, N. A., & Habib, M. M. (2019). Internal control and fraud prevention. *International Journal of Recent Technology and Engineering,* 8(3), 5556-5567.

Oduro, D. A., Okolo, J. N., Bello, A. D., Ajibade, A. T., Fatomi, A. M., Oyekola, T. S., & Owoo-Adebayo, S. F. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning. *International Journal of Science and Research Archive,* 14(3), 1412-1420.

Otley, D. (1980). The contingency theory of management accounting: Achievement and prognosis. Accounting, Organizations and Society, 5(4), 413-428. [DOI]

Pilonato, S. (2022). Accounting and corruption networks. *Journal of Public Budgeting, Accounting and Financial Management,* 34(1), 120-138.

Pizzi, S., Venturelli, A., & Macario, G. P. (2021). Digital transformation and internal auditing. Technology in Society, 67, 101738.

Popoola, O., et al. (2016). *Capability element and fraud prevention*. MPRA Paper No. 75945. https://mpra.ub.uni-muenchen.de/75945/

Rashid, M. A., et al. (2022). Corporate fraud prevention. *Australasian Accounting, Business and Finance Journal,* 16(1), 101-118.

Saudi Central Bank (SAMA). (2022). *Counter-fraud framework*. https://rulebook.sama.gov.sa

Saudi Central Bank (SAMA). (2022). *Internal control guidelines for financial institutions*. https://www.sama.gov.sa

Saudi Central Bank (SAMA). (2023). *Principles of compliance*. https://rulebook.sama.gov.sa

Sulaiman, N. A., et al. (2022). Audit rotation and governance. *Management and Accounting Review,* 21(3), 71-89. [DOI]

U.S. International Trade Administration. (2025). *Saudi Arabia - Digital economy*. U.S. Department of Commerce.

Ushakov, D., et al. (2022). Big data analytics in fraud detection. *Transportation Research Procedia,* 63, 2385-2391.

Waliullah, A., et al. (2025). *Cybersecurity in digital banking*. arXiv Preprint, arXiv:2503.22710.