European Journal of Business and Management Research
www.ejbmr.org

The Impact of Internal Control Systems on Minimizing Fraud: The Case of Lebanon

Mohamed Gaber Ghanem and Ghina Awad

ABSTRACT

Establishing reliable internal control systems in Lebanon is a challenge for businesses looking to reduce their vulnerability to fraud. The purpose of this research was to determine whether or not internal control measures were successful in reducing fraud in Lebanon's commercial sector. The study polls 308 businesses to learn more about control methods such as division of responsibilities, audit frequency, and ethics education. The results illuminate the present status of internal controls in Lebanon, illuminating the country's successes and failures in its efforts to prevent fraud. With the information from this research, businesses may improve their fraud prevention tactics and safeguard their assets in the Lebanese market.

Keywords: Controlling activities, controlling environment, information and communication, internal control, monitoring.

Submitted: August 20, 2023

Published: September 15, 2023

ISSN: 2507-1076

DOI: 10.24018/ejbmr.2023.8.5.2160

M. G. Ghanem
Department of Accounting, Alexandria University, Egypt.
(e-mail: mohamed.ghanem@alexu.edu.eg)
Ghina Awad*
Department of Accounting, Beirut Arab University, Lebanon.
(e-mail: g.awad@bau.edu.lb)

Corresponding Author

I. Introduction

Musa (2019) found that small and medium-sized enterprises (SMEs) are substantially more susceptible to losses from workers and far less likely to control these losses than big firms. Small and medium-sized enterprises (SMEs) have an easier time with internal control than giant organizations (Alayli, 2022). It is crucial to the growth of SMEs that internal control measures be used since doing so may benefit SMEs, policymakers, and support organizations. A suitable definition of SMEs would need to meet both quantitative and qualitative requirements to depict their predominance in the economy effectively (Eaton & Korach, 2016). As stated by Harasheh and Provasi (2022), the goal of fraud detection is to catch fraudulent behaviour as soon as possible so that it may be remedied (Alayli, 2022). When fraud detection measures are in place, criminals are less inclined to commit fraud since they are more likely to be discovered (Kartini, 2015). The capacity to recognize fraud is critical in investigating and preventing fraud since the extent of a fraud scheme may be considerably impacted by how fast and efficiently it is caught (Ushakov et al, 2022). To effectively combat fraud, it is necessary first to identify its potential causes (Pilonato, 2022).

II. Theoretical Framework

Here, we'll discuss the fundamental concepts that form the basis of our inquiry. The theories that guide scientific inquiry serve as a framework for researchers to define their study's parameters. This investigation is grounded on the principles of contingency theory.

A. Contingency Theory

During an audit, the auditors will perform several different tests and processes. Sub-process auditing, particularly for preparation and fieldwork, considers a wide range of factors, including the kind of organization, the level of experience of the accountants, applicable laws, the availability of audit professionals, and the technology and systems at hand. Dinh and Schultze (2022) stated that the contingency is that one thing depends on the result of another (Alayli, 2023b). Audits might be loosely organized around specific tasks. Auditors must effectively handle inspections and consider elements to fulfil their duty, which may differ significantly based on the auditing location and the kind of company pattern (Alayli, 2023c). It is possible to examine group dynamics with the help of the theory of accidental events (Hamza & Shatila, 2022). The supervisors of auditing departments are often audited themselves (Castro *et al.*, 2019). Ad hoc project audit teams are formed, and auditors are selected for auditing based on their knowledge, experience, and availability. Audit teams use a framework and a variety of planning strategies to speed up the production rollout.

B. Agency Theory

Relationships between agents and their respective governments, owners, or executives may be best described using the idea of agencies (Lowe *et al.*, 2015). When management is unsure of what to do next or does not have the time to learn the ropes, they may ask for an operator's help. A company's shareholders elect representatives to act as owners and make decisions. A business ethos should consider both the best and worst of human nature. An objective conflict of interest may arise if an agency were to transfer ownership to its management (Rametse *et al.*, 2020).

Independent thinking, it is said, the participants may help topple the operators (Rashid *et al.*, 2022). In other words, you do not do what the director and the boss want if you believe they can be persuaded only by each other and will not be swayed by other factors (Solichin *et al.*, 2022). Research on fraud analyzed the difficulties encountered by Nigerian SMEs. Sarhan *et al.* (2019) collected primary information by talking to people and asking them questions. Managers and workers at SMBs are surveyed with both closed- and open-ended questions to glean their thoughts on fraud risk management (Ushakov et al, 2022). Only 18 of the 20 people interviewed were willing to complete the questionnaire. Though it was assumed that small and medium-sized enterprises would implement fraud detection procedures, the research did not assess the performance of internal control systems.

III. Hypothesis Development

Adequate internal controls cannot be put in place without trustworthy monitoring mechanisms. Regular monitoring of processes and dealings is required to detect anomalies or warning signs early on. This may be aided by conducting frequent internal audits and reviews and using technology-based monitoring tools (Nyakarimi *et al.*, 2020). Several firms have established anonymous reporting procedures to safeguard workers who come forward with knowledge about potentially fraudulent behaviour and to encourage them to do so (Abdullatif & Al-Rahahleh, 2020). Protecting sensitive company information is an essential part of any effective EHS policy. Businesses are more vulnerable to cyber-attacks and data breaches as they become more reliant on digital technology (Ushakov & Shatila, 2022). Firewalls, encryption, and routine system upgrades are all critical components of an information security strategy to prevent data breaches. A security breach might have less of an effect if regular data backups are performed and a disaster recovery strategy is in place (Prodanova *et al.*, 2019).

Fraud prevention and detection rely heavily on environmental and strong internal controls. Organizations may get insight into their most excellent exposure points to fraud by conducting a thorough risk assessment. In prioritizing preventative actions and allocating resources efficiently, this evaluation is helpful (Berdiyeva *et al.*, 2021). Businesses may reduce fraudulent activity by educating workers, giving fraud detection training, and fostering ethical behaviour. A company's efforts to foster a culture of honesty and accountability may be aided by informing workers of the potential costs of dishonesty. Workers who get ongoing training may be better able to spot signs of fraud and other questionable conduct (*Pizzi et al.*, 2021).

In addition, businesses may use sophisticated analytics and data mining methods to uncover illegal or unethical behaviour. Overcharging customers or failing to live up to other financial commitments might be two examples of fraud that these computers could sift through to find. The use of automated fraud detection technologies may improve organizational effectiveness and accuracy in avoiding fraud (Grayston, 2022).

H1: There is a significant relationship between controlling the environment and fraud prevention.

Constant vigilance over internal controls is required while evaluating production. Extensive testing is required to verify whether or not natural internal control systems are compatible and whether or not additional threats may be neutralized (Fulop *et al.*, 2018). Companies nowadays rely heavily on information and communication networks to store and disseminate massive amounts of organizational, financial, and regulatory data to help effectively administer corporate operations. Information on external operations is as significant as information on internal operations when making a company decision (Alberti *et al.*, 2022).

Joint monitoring and fraud prevention efforts may provide better results. Experts in fraud prevention, forensic accounting, or external auditing may be called in to assist in getting an unbiased perspective on the issue. Third parties can conduct audits, evaluate internal control systems, and provide suggestions to bolster fraud protection measures. Lastly, monitoring is a powerful tool in the war against fraud (Sulaiman *et al.*, 2022). By putting in place thorough monitoring systems, businesses have a better chance of preventing additional losses of money and goodwill due to fraudulent actions. To effectively monitor and prevent fraud, it is necessary to review financial transactions often, apply data analytics tools, maintain eyes on employee activity, and coordinate with external stakeholders. Businesses may protect their assets and reputation against fraud by promoting a culture of awareness and responsibility (Rendon & Rendon, 2015).

H2: There is a significant relationship between monitoring and fraud prevention.

According to (Hay et al., 2020), improved information and communication infrastructure should accelerate the dissemination of academic results. Risk assessment tasks in internal control include identifying, evaluating, and monitoring internal controls in response to potential threats. The intentional or unintentional misrepresentation or abuse of financial data significantly compromises the effectiveness of a property's operations. The impact of internal control on output variables has also been the subject of observational research. Internal controls have been linked to favourable results in some of these studies, while negative results have been found in others. Harber and Marx (2020) draw the following conclusion from their research: internal controls are highly correlated (r = 0.818) with the effectiveness of financial management. Agustina *et al.* (2021) looked at internal control measures in Uganda's higher education industry and concluded that they had a significant impact on preventing fraud. Organizations may reduce their vulnerability to fraud by fostering a culture of openness and accountability via open lines of communication. All staff must be well-versed in the company's ethics and fraud prevention standards. Employees may learn about the effects of fraud and their involvement in preventing and reporting it via ongoing training and awareness initiatives. To promote the reporting of suspicious actions without fear of punishment, open channels of communication between management and staff are crucial (Ozili & Outa, 2019).

Combating fraud in the workplace calls for an atmosphere where employees feel comfortable talking to one another and sharing their views. Organizations may encourage honesty and integrity by implementing robust information management systems, encouraging open dialogue, and supporting effective lines of communication. Anonymous reporting techniques, regular training, and cross-sector cooperation may all contribute to better information and communication in the fight against fraud. Businesses may protect their assets, reputation, and long-term sustainability against fraud by regularly evaluating and enhancing these areas.

H3: There is a significant relationship between information and communication and fraud prevention.

No possible risk is too remote for Risk Identification to look into, regardless of how it relates to the company's typical activities or declared objective. Both quantitative and qualitative metrics will be used to determine success. Managers at the top must consider how their teams interact with one another and the outside world (Alayli, 2023a). Management planning conferences, strategic planning, routine evaluations of the aspects of an agency's activities, shifting demands or expectations from agency officials or the public, and natural disasters are just some of the ways the risk might be uncovered (Ozili & Outa, 2018). Management should undertake a risk analysis after identifying hazards at the task and division levels. Employee input throughout the risk assessment process is crucial. Employees are often the first line of defense against fraud because of their proximity to day-to-day operations (White *et al.*, 2020). The best method for firms to include their personnel is to solicit feedback, make it simple for workers to report suspicious conduct, and encourage them to look for potential dangers. Consistent training and awareness programs may help employees understand their role in combating fraud and developing an ethical culture (Nyambuya *et al.*, 2021). While doing a risk assessment, it might be beneficial to consult with outside parties, including industry associations, law enforcement, and independent auditors. Businesses may better spot threats and implement preventive measures by comparing notes with competitors, learning from best practices, and analyzing industry benchmark data. The reporting and investigation of fraud may be sped up by collaborating with local authorities (Millet-Reyes & Uddin, 2021).

In conclusion, every severe business about avoiding fraud should do a comprehensive risk assessment. By conducting in-depth risk assessments, businesses may better prepare for and react to threats, optimize resource allocation, and strengthen security in general. In today's ever-changing economic context, fraud prevention strategies can only succeed if constantly evaluated and tweaked. Engaging employees and forming partnerships with external stakeholders to enhance risk assessment methods and establish a solid fraud prevention framework may help organizations better defend their assets, reputation, and long-term sustainability against fraud.

H4: There is a significant relationship between risk assessment and fraud prevention.

Good communication and training are essential for controlling activities to prevent fraud. Clear communication of rules, procedures, and control requirements will equip workers to prevent and detect fraud. Training programs may help workers understand the significance of internal controls, identify fraud risks, and understand the effects of fraudulent behaviour. A culture of integrity and accountability may improve the possibility that employees will comply with control activities and report those that seem suspicious (Baker *et al.*, 2017). The success of control efforts relies on regular monitoring and assessment. Regular internal audits, independent reviews, and evaluations by external experts are all effective ways for businesses to identify control flaws and fill them up. By doing such a review, firms may be better prepared to combat emerging fraud threats (Jalloul *et al.*, 2022).

Collaboration with external stakeholders, such as external auditors and industry associations, to glean ideas and best practices may assist in controlling activities for fraud prevention. External auditors may assess internal controls' effectiveness and provide enhancement recommendations. Control systems may be improved with the help of trade associations via data sharing and comparison to best practices (Shatila & Alozian, 2019). Activity control is a vital instrument in every company's arsenal against fraud. By implementing measures such as job segregation, robust internal controls, the use of technology, open lines of communication and training, and regular reviews, businesses may strengthen their control systems and decrease the possibility of fraudulent activities. Businesses can safeguard their resources, standing in the community, and future success by fostering a culture of trust, transparency, and accountability.

H5: There is a significant relationship between controlling activities and fraud prevention.

IV. Methodology

This section provides guidelines that specify the approach used to investigate the relationship among the variables, identify the purpose of the research, demonstrate how data is collected, define the population, its size, and the analysis techniques used.

The methodologies used in this study were strictly quantitative. Analyses and measurements can't function without ratios. Analysis of variance, correlation, and regression are only a few statistical approaches used to summarize the findings of quantitative studies. Methods that can be promptly evaluated and implemented at little expense are more likely to be used. The first step in data organization is choosing a suitable measurement scale. In academia, deductive and inductive reasoning are the two primary research strategies. The primary distinction between studies is the methodology used. Deductive research strives to prove an existing notion instead of inductive research, which seeks to generate a new hypothesis.

After collecting and evaluating data, we used the deductive method to probe a hypothesis tested in other countries and to put theories gleaned from the literature to the test. The primary goal is to look into some questions concerning a

fresh, unknown angle on the topic. Based on the results of an exploratory study, it may be feasible to conduct a more in-depth study, or it may not. To answer research questions and test hypotheses, researchers must systematically gather and analyze data on the relevant variables of interest. Primary and secondary sources make up the backbone of the information ecosystem. The study relied heavily on in-person interviews and questionnaires. We used a questionnaire to get responses from real people. For each item in the questionnaire, respondents indicated their degree of agreement or disagreement using a Likert scale, often a five-point scale. The participants were given a scale on which to rate their level of agreement with each statement. Lebanese small and medium-sized enterprise accountants and auditors are the typical responders to such surveys.

V. Measuring Variables

The primary goal of this research was to examine the connections between the many components of an efficient fraud prevention strategy (controlling environment, monitoring, information and communication, risk assessment, and control actions).

The Controlling Environment Scale (Meiryani *et al.*, 2019) consists of three questions. The company has a system in place to ensure the controls detailed in the manuals are really being used, and it reviews and updates its policies and procedures regularly.

As part of the five-point Monitoring Scale created by Fung *et al.* (2022), statements like "*Staff are required to sign off, indicating their performance of critical control activities like performing reconciliations*" and "*Accountants understand their obligation to communicate observed weaknesses in design with the internal control structure of the organization to the appropriate supervisory personnel*" are included.

The four questions used to evaluate "Information and Communication" as an independent variable were taken directly from Castro *et al.* (2019) It was stated that operational and financial information is communicated, that a process is in place to collect information from external sources that could impact the organization and the financial reporting process, and that milestones to achieve financial reporting objectives are monitored to ensure that timing deadlines are met.

Some questions used to quantify the independent variable Risk Assessment included the possibility of financial statement deception and the steps taken to mitigate that possibility.

The three-question Controlling Activities measure developed by Oradi *et al.* (2020) was utilized for this study. Participants were asked to score the accuracy of the following statements: "*Operational accountability and record-keeping responsibilities are distinct,*" "*Custody over assets is separate from accounting,*" and "*Prompt and appropriate follow-up action is performed on exception reports*."

Castro *et al.* (2019) created a scale to quantify the idea of Fraud Prevention, including things such as that without adequate internal controls, fraud is rampant, having such controls in place improves financial outcomes, and so on.

A. Data Analysis and Hypothesis Testing

Sections covering demographic factors, research variable descriptions, validity and reliability statistics, regression analysis, and ultimately, Pearson correlations followed the data analysis and hypothesis testing.

B. Reliability Analysis

The following section of the university will address the reliability analysis using the Cronbach Alpha indicator.

VI. Regression Analysis

This section addressed the regression analysis, which is a statistical test used to validate the research hypothesis based on a margin error of 5%. If the $P < 0.05$, then H0 is rejected, and H1 is accepted, and vice versa.

TABLE I: Regression Analysis

Variable in the model	Coefficient (B)	p-value
(Constant)	0.716	0.000
Risk Assessment	0.596	0.001
Controlling Activities	0.434	0.002
Controlling Environment	0.193	0.004
Monitoring	0.238	0.007
Information & Communication	0.329	0.000

Table I offers valuable insights into the relationship between various predictor variables and the dependent variable, Fraud Prevention. The Model Summary section indicates that the model as a whole demonstrates a moderate positive correlation ($R = 0.564$) between the independent variables and the dependent variable. The R-squared value of 0.318 suggests that approximately 31.8% of the variance in Fraud Prevention can be explained by the independent variables. The adjusted R-squared of 0.296 adjusts for the number of predictors and indicates that the model's explanatory power remains reasonable while guarding against overfitting. The standard error of the estimate (0.937) provides an estimate of the variability in Fraud Prevention not accounted for by the model.

The coefficients, their standard errors, t-values, and significance levels in the Unstandardized Coefficients section shed light on the specific impact of each predictor variable. Notably, all predictor variables—Risk Assessment, Controlling Activities, Controlling Environment, Monitoring, and Information and communication—appear to be statistically significant predictors of Fraud Prevention, as indicated by their p-values (Sig.) being below 0.05. This suggests that these predictors play a role in predicting Fraud Prevention.

From these results, it is possible to construct a regression equation to predict Fraud Prevention based on the predictor variables. The equation takes the form:

$$\text{Fraud Prevention} = 0.716 + (0.596 \times \text{Risk Assessment}) + (0.434 \times \text{Controlling Activities}) + (0.193 \times \text{Controlling Environment}) + (0.238 \times \text{Monitoring}) + (0.329 \times \text{Information \& Communication})$$

This equation allows for predictions of Fraud Prevention based on the values of the predictor variables.

Upon analyzing the equation, several insights emerge. The intercept (0.716) represents the expected value of Fraud

Prevention when all predictor variables are zero. Positive coefficients indicate that increasing the corresponding predictor variable is associated with higher Fraud Prevention values. Among the predictors, Risk Assessment has the most substantial impact, as indicated by its coefficient of 0.596. The t-values reflect the statistical significance of each predictor's contribution. It's important to keep in mind that these findings rest on the assumption of a linear relationship between predictors and the dependent variable, and it's advisable to assess the model's assumptions and validate its results in context. In conclusion, this regression analysis offers a valuable framework for understanding how these predictor variables collectively influence Fraud Prevention.

VII. Discussion

Since it has been shown that monitoring frameworks affect performance evaluations, the relevance of modern-day firms' reliance on monitoring systems has only increased. The company's culture has a significant impact on the viewpoint of the management team. It is possible to build additional levels of internal control on top of the base supplied by the monitoring system. Boards of directors or audit committees, management philosophies, and organizational styles need total autonomy to establish, execute, and supervise policies effectively.

For this reason, the study examines not only the ethics and ethical beliefs of the individuals in charge of setting and implementing controls but also the culture and working style of the organizations themselves. A complex set of factors regulates our natural environment. The board of directors has tasked members of the executive board and several board committees with preparing this report. Internal regulation, they argue, is to fault if like factors are treated similarly. They strengthen the system as a whole by providing more structural support.

The absence of a systematic mentorship program has contributed to the widespread lack of organizational discipline from the dawn of management. The audit committee is now seen in a more nuanced light as a source of knowledge by most organizations. Board monitoring is still needed, even if boards of directors pay less attention to institutional problems. The board of directors should consider internal control measures for more than merely facilitating efficient operations behind the scenes.

Constant monitoring of internal controls is required while assessing productivity. Extensive testing is necessary to assess the manageability of new risks and the compatibility of internal control systems. Data such as financial, operational, and regulatory information, among others, are stored and organized by businesses through information and communication networks. When making business choices, it's essential to look within and outside.

There may be efficiencies gained in data collection and dissemination via ICTs. It is possible to measure the effectiveness of internal controls by identifying, analyzing, and monitoring preexisting procedures designed to mitigate risks. The spread of false or misleading financial information about a property may have a disastrous impact on its capacity to function normally.

Observational studies have also examined the link between internal control and output variables. Most of these studies find a positive association between internal controls and findings, while others find either no interaction at all or just a weak link.

Threats to the organization's capacity to achieve its mission, not simply those identified in the risk assessment, will be carefully examined. Actions' non-monetary drivers would be taken into account. The management group has to consider how the various divisions and external factors influence one another. Management planning conferences, strategic planning, periodic inspections of department activity aspects, fluctuating demands or expectations from agency officials, and public and natural catastrophes are all possible tactics for detecting the risk.

When management becomes aware of risks at the activity or departmental levels, they should conduct a risk assessment. Low probability and low-impact threats may not be the cause for significant worry. Before making a decision, management must weigh the severity and likelihood of the danger. While there are various ways to achieve this goal, all organizations should be constructed to resist risk within the limitations set by management. The therapy's effectiveness must be thoroughly assessed before it may be used.

As companies grow, their approaches to risk management evolve. Management must constantly monitor progress throughout implementation to ensure that all potential threats are mitigated. Most controls, however, may be categorized into two groups: those that aim to detect issues and those that aim to prevent them. Precautions are made to lessen the potential for trouble. One of the most critical aspects of creating these safeguards is anticipating and avoiding potential problems. Adverse events may be tracked in real time and reported to superiors. The price of prevention is often higher than the price of discovery. The benefits and drawbacks of preventive measures must be considered before they are used. Management should also remember that adding too many new safety measures at once might reduce efficiency. There is no foolproof method of lowering the odds of terrible things happening. An alternative control measure may be used in certain situations instead of requiring a blend of measurements.

VIII. Recommendations

1) Conducting a comprehensive review of the company's procedures, processes, and systems to look for signs of fraud,

2) Determining which threats are most important based on their potential impact and severity,

3) Setting up a reliable system of internal controls: Establishing and recording policies, procedures, and controls for all processes and divisions,

4) Ensuring a clear separation of responsibilities so unapproved actions and collaboration may be avoided,

5) Using cutting-edge technology, such as data analytics tools, automated systems, and monitoring software, in the fight against fraud,

6) Using data analysis in real-time to prevent and detect fraud,

7) Consistently monitoring business operations, monetary transactions, and financial reports for signs of fraud,

8) Using automatic alerts and exception reporting to spot signs of possible fraud immediately,

9) Conducting regular internal audits and reviews to guarantee the efficacy of control efforts,

10) Encouraging honest conduct and education on the dangers of fraud in the workplace,

11) Giving your employees consistent instruction and updates on fraud prevention, control, and reporting initiatives,

12) Inspiring the staff to come forward with any suspicious activity reports without worrying about repercussions,

13) Encouraging workers, customers, and stakeholders to report suspicious or concerns about fraudulent activity by establishing transparent and confidential reporting tools like hotlines or online platforms,

14) Keeping up with the ever-evolving fraud threats and new technology by regularly reviewing control actions

15) Remaining updated on the field's latest best practices, laws, and fraud detection methods,

16) Constantly assessing and improving control systems to fill any control gaps or shortcomings,

17) Consulting independent auditors, trade groups, and law enforcement for advice on managing operations and preventing fraud,

18) Joining relevant industry forums and data-sharing platforms to keep up with the latest fraud trends,

19) Motivating employees from all levels to watch for fraudulent activity and take preventative measures,

20) Developing an organizational culture that values and publicly acknowledges workers who assist with anti-fraud initiatives,

21) Promoting experimentation and new approaches to regulate activities,

22) Providing continuous professional development and training to those responsible for monitoring activities and preventing fraud,

23) Keeping abreast of new controls, methods, and technologies to prevent fraud as they become available.

By adopting these suggestions, organizations may improve their control operations and fraud prevention efforts. A proactive and all-encompassing strategy for managing operations is essential when safeguarding the organization's assets, reputation, and long-term sustainability against fraud dangers.

IX. LIMITATIONS

People may still make errors or work together to avoid detection, even with restrictions. There is always the possibility of fraud or theft on the part of workers, and no control mechanism is foolproof. Investments in technology, training, and monitoring systems are sometimes necessary to implement and sustain effective control operations. The potential advantages of fraud prevention must be weighed against the expenses of control measures. Constantly innovating new and complex methods, fraudsters find ways to evade detection and prevention efforts. It might be difficult for businesses to detect new fraud patterns and adjust their internal controls quickly. Technology may improve control operations, but its flaws, such as cybersecurity holes or the chance for false positives or negatives in automated monitoring systems, must be considered. Technology should not be considered a panacea but rather a tool that aids in the execution of control measures.

Employees who are used to the status quo or see the new procedures as onerous may push back against implementing control activities. When workers refuse to accept or follow new control measures, the efficacy of the control system suffers. Consistent execution of control operations across the board may be complex for large firms with many divisions, offices, and subsidiaries. It might be challenging to build unified control systems due to the complexity of coordinating and communicating across several business groups. The potential for fraud and the efficiency of control efforts may be affected by circumstances outside of the organization, such as the state of the economy, industry-specific hazards, or changes in rules. Businesses must be watchful and modify their control systems to account for unpredictable environmental variables. Professionals who can plan, administer, and monitor control operations are crucial to any anti-fraud effort. Smaller firms may struggle to acquire the necessary resources and skills in fraud prevention.

Even though controls may lessen the likelihood of fraud, they cannot eliminate it. When it comes to addressing new and evolving fraud threats, it is imperative that organizations avoid complacency and continually examine, update, and test their control systems. Some workplace cultures may discourage employees from reporting fraud issues out of fear of reprisal or a lack of faith in the reporting processes. The key to success in these obstacles is fostering an environment where honesty and integrity are valued. To successfully handle fraud threats, businesses must be aware of these constraints and regularly analyze and enhance their control operations. When combined with regular monitoring and evaluation, a proactive and adaptable strategy for preventing fraud may help businesses overcome these obstacles.

REFERENCES

Abdullatif, M., & Al-Rahahleh, A. S. (2020). Applying a new audit regulation: Reporting key audit matters in Jordan. *International Journal of Auditing*, *24*(2), 268–291.

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.

Alayli, S. (2022). The impact of internal control practices on fraud prevention: The case of Lebanese small-medium enterprises. *European Journal of Business and Management Research*, *7*(5), 141-147.

Alayli, S. (2023a). The impact of capital budgeting practices on financial performance of Lebanese banks. *The EUrASEANs: Journal on Global Socio-economic Dynamics*, *1*(38), 29-39.

Alayli, S. (2023b). The impact of digital banking on customer satisfaction in the Lebanese banking industry: The mediating effect of user experience. *International Journal of Information Management Sciences*, *7*(1), 1-22.

Alayli, S. (2023c). The mediating effect of metaverse technology on the relationship between virtual economy and launching clothing retailers: The case Of Dubai. *Journal of Positive Psychology and Wellbeing*, *7*(2) 1707-1717.

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.

Baker, C. R., Cohanier, B., & Leo, N. J. (2017). Breakdowns in internal controls in bank trading information systems: The case of the fraud at Société Générale. *International Journal of Accounting Information Systems*, *26*, 20–31.

Berdiyeva, O., Islam, M. U., & Saeedi, M. (2021). Artificial intelligence in accounting and finance: Meta-analysis. *NUST Business Review*, *3*(1), 56–79.

Castro, P. R., Amaral, J. V., & Guerreiro, R. (2019). Adherence to the compliance program of Brazil's anti-corruption law and internal controls implementation. *Revista Contabilidade e Financas*, *30*(80), 86–201.

Dinh, T., & Schultze, W. (2022). Accounting for R&D on the income statement? Evidence on non-discretionary vs. discretionary R&D capitalization under IFRS in Germany. *Journal of International Accounting, Auditing and Taxation*, *46*, 1-20.

Eaton, T. V, & Korach, S. (2016). A criminological profile of white-collar crime. *Journal of Applied Business Research*, *32*(1), 129–142.

Fulop, M. T., Tiron-Tudor, A., & Cordos, G. S. (2018). Audit education role in decreasing the expectation gap. *Journal of Education for Business*, *94*(5), 306–313.

Fung, S., Pham, V. T., & Raman, K. K. (2022). Client corruption culture and audit quality: the conditioning effect of the competitive position of the incumbent auditor. *Review of Quantitative Finance and Accounting*, *59*(3), 1133–1171.

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

Harasheh, M., & Provasi, R. (2022). A need for assurance: Do internal control systems integrate environmental, social, and governance factors? *Corporate Social Responsibility and Environmental Management*, *30*(1), 384-401.

Harber, M., & Marx, B. (2020). Auditor independence and professional scepticism in South Africa: Is regulatory reform needed? *South African Journal of Economic and Management Sciences*, *23*(1), 1-12.

Hamza, I., & Shatila, K. (2022). The Effect of Gamification on Employee Behavior: The Mediating Effects of Culture and Engagement. *The Journal of Asian Finance, Economics and Business (JAFEB)*, *9*(5), 213-224.

Hay, D., Shires, K., & Van Dyk, D. (2020). Auditing in the time of COVID – the impact of COVID-19 on auditing in New Zealand and subsequent reforms. *Pacific Accounting Review*, *33*(2), 179–188.

Jalloul, S., Awwad, G., & Shatila, K. (2022). The impact of accounting information systems on bank performance: The case of Lebanon. *Management and Economics Review*, *7*(3), 405-422.

Kartini, K. (2015). Accountability mediation effect on internal control effect against fraud prevention (A study in the government of West Sulawesi, Indonesia). *International Journal of Economic Research*, *12*(1), 195–204.

Lowe, D. J., Pope, K. R., & Samuels, J. A. (2015). An examination of financial sub-certification and timing of fraud discovery on employee whistleblowing reporting intentions. *Journal of Business Ethics*, *131*(4), 757–772.

Meiryani, M., Fitriani, N. A., & Habib, M. M. (2019). Can information technology and good corporate governance be used by internal control for fraud prevention? *International Journal of Recent Technology and Engineering*, *8*(3), 5556–5567.

Millet-Reyes, B., & Uddin, N. (2021). Board structure changes after accounting fraud: the case of Schneider Electric. *CASE Journal*, *17*(3), 406–418.

Musa, N. (2019). A conceptual framework of IT security governance and internal controls. *Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik*, *7*(2), 63-77.

Nyakarimi, S. N., Kariuki, S. N., & Kariuki, P. W. (2020). Application of internal control system in fraud prevention in banking sector. *International Journal of Scientific and Technology Research*, *9*(3), 6524–6536.

Nyambuya, K., Yasseen, Y., & Soni, F. (2021). Barriers to the adoption of independent reviews by nonpublic interest entities in South Africa. *African Journal of Business and Economic Research*, *16*(2), 185–206.

Oradi, J., Asiaei, K., & Rezaee, Z. (2020). CEO financial background and internal control weaknesses. *Corporate Governance: An International Review*, *28*(2), 119–140.

Ozili, P. K., & Outa, E. R. (2018). Bank income smoothing in South Africa: role of ownership, IFRS and economic fluctuation. *International Journal of Emerging Markets*, *13*(5), 1372–1394. https://doi.org/10.1108/IJoEM-09-2017-0342

Ozili, P. K., & Outa, E. R. (2019). Bank earnings smoothing during mandatory IFRS adoption in Nigeria. *African Journal of Economic and Management Studies*, *10*(1), 32–47.

Pilonato, S. (2022). Accounting can support a "sustainable" corruption network: a case analysis. *Journal of Public Budgeting, Accounting and Financial Management*, *34*(1), 120–138.

Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. *Technology in Society*, *67*(101738).

Prodanova, N. A., Trofimova, L. B., Bashina, O. E., Kachkova, O. E., Ilienkova, N. D., & Polyanskaya, T. A. (2019). Approaches for obtaining audit evidence at fair value measurement. *International Journal of Economics and Business Administration*, *7*(3), 279–292.

Rametse, N., Makara, T., & Santhariah, A. (2020). An investigation of the attitudes of business taxpayers towards the Malaysian goods and services tax and its potential managerial benefits. *Journal of the Australasian Tax Teachers Association*, *15*, 115–141.

Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting, Business and Finance Journal*, *16*(1), 101–118.

Rendon, R. G., & Rendon, J. M. (2015). Auditability in public procurement: An analysis of internal controls and fraud vulnerability. *International Journal of Procurement Management*, *8*(6), 710–730.

Sarhan, A. A., Ntim, C. G., & Al-Najjar, B. (2019). Antecedents of audit quality in MENA countries: The effect of firm- and country-level governance quality. *Journal of International Accounting, Auditing and Taxation*, *35*, 85–107.

Shatila, K., & Alozian, M. (2019). Factors affecting employee turnover: the case of Lebanese retail companies. *Journal of Human Resources*, *7*(2), 5-13.

Solichin, M., Sanusi, Z. M., Johari, R. J., Gunarsih, T., & Shafie, N. A. (2022). Analysis of audit competencies and internal control on detecting potential fraud occurrences. *Universal Journal of Accounting and Finance*, *10*(1), 171–180.

Sulaiman, N. A., Jaffar, N., & Yahya, Y. (2022). Audit rotation and strength of corporate governance and its effects on audit quality. *Management and Accounting Review*, *21*(3), 71–89.

Ushakov, D., & Shatila, K. (2022). The impact of engagement on turnover intention: The case of United Arab Emirates banks. *The EUrASEANs: Journal on Global Socio-economic Dynamics*, *5*(36), 94-105.

Ushakov, D., Dudukalov, E., Mironenko, E., & Shatila, K. (2022). Big data analytics in smart cities' transportation infrastructure modernization. *Transportation Research Procedia*, *63*, 2385-2391.

Ushakov, D., Dudukalov, E., Shmatko, L., & Shatila, K. (2022). Artificial Intelligence as a factor of public transportations system development. *Transportation Research Procedia*, *63*, 2401-2408.

White, S., Bailey, S., & Asenova, D. (2020). Blurred lines: exploring internal auditor involvement in the local authority risk management function. *Public Money and Management*, *40*(2), 102–112.