ZIBELINE INTERNATIONAL™ PUBLISHING

ISSN: 2821-2983 (Online)
CODEN: MBMJAO

Malaysian Business Management Journal (MBMJ)

DOI: http://doi.org/10.26480/mbmj.01.2025.20.32

RESEARCH ARTICLE

IMPLEMENTATION OF INTERNAL CONTROL SYSTEMS ON FRAUD PREVENTION AND DETECTION IN RURAL BANK OF BATANGAS

Johanah P. Alisen

San Pablo Colleges, San Pablo City, Philippines.
**Corresponding Author Email: johanahalisen.mba@gmail.com*

ARTICLE DETAILS

Article History:

Received 03 January 2025
Revised 13 January 2025
Accepted 18 February 2025
Available online 15 March 2025

ABSTRACT

The potential of fraud is one of the typical governance concerns faced by monetary institutions, such as rural banks, regardless of size, location, or operational complexity. Having robust internal control systems and establishing a risk management program is critical in combating fraud. This study explores the implementation of Internal Control Systems of the firm RB concerning the principles prescribed by the COSO framework. The research method used in the study was quantitative. The participants of the study comprised 55 stakeholders of the institution selected based on purposive sampling. Findings show that the business has internal control systems in place which are generally implemented to a great extent as prevention and detection controls. The recommendation includes that the company should consider studying and investing in fraud prevention software and designs, integrating its best practices and existing regulatory standards with technological advancements to combat new probable fraud schemes.

KEYWORDS

Internal control systems, prevention, and detection, stakeholders, implementation

1. INTRODUCTION

Financial institutions are exposed to fraud risk which can result in monetary losses, reputational damage, and regulatory penalties. Fraud can be classified into three types, namely, internal or occupational fraud, external fraud, and fraud against individuals. Occupational fraud is a type of fraud that exists within the organization. According to Associate of Certified Fraud Examiners (ACFE) *Occupational Fraud 2024: A Report to the Nations*, 138 countries have reported a total of 1,921 fraud cases that resulted in losses greater than 3.1 billion dollars. Approximately 5% of an organization's annual revenue is assumed to be lost due to workplace fraud. Furthermore, the study identified banking and financial services as having the most exposure to occupational fraud, with 305 cases or an average loss of $120,000.00 globally. According to PwC's 2020 Global Economic Crime and Fraud Survey: The Philippine Report, businesses experienced an average loss of $100,000 from fraud incidents in the last 24 months, with 38% of these cases originating internally.

Fraud is a crime waiting to happen and is caused by human involvement, rather than chance. To minimize the occurrence of fraud and its impact, the implementation of strong internal control systems is critical to mitigating fraud risk by establishing frameworks that safeguard assets, guarantee accuracy in financial reporting, and encourage compliance with legal requirements. The COSO framework lays the foundation of the mandatory standards for businesses to execute the suitable internal control procedures through establishing a robust internal control design. The framework involves all five components, namely the control environment, risk assessment, control activities, information and communication, and monitoring. However, for internal control to achieve its aims, it is necessary to understand why fraud happens and why people commit such acts. The fraud diamond serves as a framework to comprehend the motivations behind fraud so that internal control can succeed the objective of detecting and preventing fraud (Abei, 2021).

A sound internal control system for fraud prevention and detection has the following advantages for an organization: early detection of issues, cost-saving benefits, reputation and credibility, compliance with laws and regulations, and operational efficiency. Despite the recognized importance of internal controls, the effectiveness of their implementation in fraud prevention and detection differs from one organization to another. This raises the question of what factors contribute to successful implementation and how these systems can be optimized to fulfill their intended role better. This research aims to investigate the existence and extent of implementing internal control systems and designs for detecting and preventing potential schemes within the bank.

2. LITERATURE REVIEW

2.1 Description of Internal Control

There is no correct method to define internal control since internal control functions vary that are applied differently across various institutions. Generally, internal control systems begin as internal processes with the purpose of assisting institutions in achieving their set objectives (Kabuye et al., 2019). American Institute of Certified Public Accountants [AICPA] (2018) defines internal control as the process of ensuring achievement of your objectives in operational effectiveness and efficiency, reliable financial reporting, adherence to laws, and regulations and policies. Whereas COSO (2013) defines internal control as a procedure carried out by an entity's board of directors, management, and other personnel, intended to give a reasonable level of assurance regarding the achievement of objectives in the following areas: (1) Effectiveness and efficiency of operations; (2) Reliability of financial reporting; and (3) Compliance with relevant laws and regulations.

Through internal control, an organization can monitor its business operations to develop secure and successful practices (Nugraha and Bayunitri, 2020). There are several benefits that internal control gives to an entity, including giving management more assurance about the accomplishment of objectives, giving insight into how well an organization

Quick Response Code	Access this article online	
	Website: www.mbmj.com.my	**DOI:** 10.26480/mbmj.01.2025.20.32

Cite The Article: Johanah P. Alisen(2025). Implementation of Internal Control Systems on Fraud Prevention and Detection in Rural Bank of Batangas. *Malaysian Business Management Journal, 4(1): 20-32.*

is performing, and assisting in the reduction of risks that could compromise the accomplishment of the organization's compliance objectives. (AICPA, 2020). The COSO framework was created to plan, carry out, and assess internal control.

2.2 The COSO Framework

To fight corporate fraud, five private sector organizations joined forces in 1985. and established The Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO is committed to enhancing organizations' performance by creating thought leadership that improves internal controls for organizational governance, business ethics, enterprise risk management, fraud, and financial reporting. It has established an internal control model that organizations may use to evaluate their internal controls. The COSO integrated framework was introduced in 1992 as a paradigm for designing, implementing, performing internal controls, and evaluating their performance. COSO (2013) highlights that an organization's administration must meet all five internal control components before determining that its system is successful. Furthermore, these five components must be "present" and "functional" in the internal control system. Being "present" signifies that the components are included in the design of the institution's internal control system, whilst being "functional" suggests that they are actively used in the institution's operations and control procedures. To be effective, the five components of internal control (control environment, risk assessment, control actions, information and communication, and monitoring) must function together in an integrated manner.

2.2.1 Control environment

The control environment, as defined by COSO (2013), provides the basis upon which internal control is performed concerning the organization's internal control system design, procedures, and standards. Moreover, the Fraud Risk Management Guide of COSO and ACFE (2023) adds that an internal control environment fosters the discipline that enables the assessment of risks to achieve the organization's goals. The control environment is comprised of human elements related to the management philosophy, dedication to competency, and the growth of integrity and ethical ideals. (Ilyas et al., 2021). Thus, COSO (2013) describes that efficacy requires a firm's dedication to ethical values and integrity, including the independence of the board of directors, who play a pivotal role in the control environment. In order to achieve goals, management should also set up reporting lines, structures, and roles under the board's direction Also, the organization should commit to attracting, developing, and retaining competent individuals in line with objectives. Individuals should be held accountable for their internal control responsibilities to meet set objectives.

2.2.2 Risk assessment

Risk assessment is a continuous and iterative process in which management identifies and evaluates risks to meet its goals (COSO, 2013). Disclosure of risk assessment roles enables investors to decide whether to invest in the institution (Ashfaq and Rui, 2019). According to a study risk assessment entails a two-step approach to risk management (Ashfaq and Rui, 2019). Identifying the company's key risks should be the first step, followed by developing strategies to manage those risks. According to COSO (2013), organizations should establish specific goals to detect and evaluate hazards linked with the goals to accomplish successful risk assessment. In order to evaluate and account for any possible fraud, it is also necessary to determine the source of the risk.

2.2.3 Control Activities

Control actions are the steps put in place by policies and procedures that aid in ensuring orders of the management to mitigate risks and attain its objectives. (COSO, 2013). In addition, this is accomplished when companies possess guidelines that specify what is required and procedures that implement policies (COSO, 2013). Maulidi and Shonhadji (2020) emphasize the significant role segregation played by duties and job rotation in reducing occupational fraud. As stated by a group study control activities guarantee that risk management is regulated utilizing the two-step approach (Ashfaq and Rui, 2019). These include choosing an applicable framework and planning mechanisms to handle risks detected with evaluation.

2.2.4 Information and Communication

Firms increasingly rely heavily on information and communication networks to store and distribute massive amounts of organizational, financial, and regulatory data, allowing them to successfully manage corporate operations. When making a business choice, information on both internal and external operations is equally important (Alberti et al., 2022). Hence, communication occurs both within and outside the organization, and it provides companies with the necessary data to carry out their controlling activities and accomplish their goals (COSO, 2013). During communication, employees can learn about operational control duties and their value in attaining purposes (Le et al., 2020). As a result, organizations created and acquired pertinent, high-quality to aid the operation of internal controls. In order to effectively manage internal control, COSO (2013) stipulates that businesses must communicate clear objectives and roles for both internal and external control.

2.2.5 Monitoring Activities

IAASB (2018) defines monitoring as activities for detecting and correcting weaknesses in the efficacy of controls across operations concerning economic instruments. Accordingly, COSO (2013) states that effective control involves a continuous and autonomous evaluation of internal control. Based on the review, the organizations shall correspond internal control efficiency to responsible personnel who can take remedial measures.

2.3 How is the COSO Framework used?

Publicly traded corporations and accounting and financial institutions extensively use the COSO Framework. The framework aims to codify how key business operations are carried out by implementing internal controls. This focuses on risk assessment and management while assisting firms in complying with legal and ethical requirements. In addition to integrating such controls into key business processes, the framework emphasizes monitoring and reporting, especially regarding using internal auditors to ensure that established controls are adhered to. (Posey, 2021)

2.4 Definition of fraud

Fraud is an international concern that impacts businesses all over the world. (2020 ACFE). Any behavior that employs dishonesty to gain an advantage is considered "fraud." According to Black's Law Dictionary, fraud is defined as the deliberate misrepresentation of the truth or the concealing of a material fact in order to influence another person to act in a way that is detrimental to that person. To put it another way, we are engaging in fraud whenever we tell lies to deprive someone or an organization of their money or property. (ACFE 2023). Similarly, the Institute of Internal Auditors' International Professional Practices Framework (2021) explains that fraud is any unlawful act that involves deception, concealment, or a breach of trust. Physical force or the threat of violence are not necessary for these actions. Fraud is committed by people and organizations in order to obtain funds, assets, or services; to escape payment or service termination; or to gain personal or competitive gain.

As noted, fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain. The Association of Certified Fraud Examiners (ACFE 2024) defines occupational fraud as using one's occupation for personal enrichment through deliberate misuse or misapplication of the employing organization's resources or assets. In PricewaterhouseCoopers' (PwC) 2020 Global Economic Crime and Fraud Survey: The Philippine Report, asset misappropriation fraud is identified as the most experienced fraudulent scheme to Philippine businesses and is the number one threat since 2016. Bribery and corruption rank as the Philippines' second most disruptive economic crime.

2.5 Why Do People Commit Fraud?

Identifying the factors that can contribute to fraud is a crucial first step in identifying and ultimately combating it. (SACFE, 2018). Studies show that an individual is more likely to commit fraud when there is an incentive (pressure), an opportunity caused by weak controls or oversight, and a justification (rationalization) behind the fraudulent behavior. These three factors are commonly known as the "fraud triangle". This model was formulated by Donald R. Cressey in 1953. Professionals widely use this concept to combat fraud by explaining conditions that could influence individuals to commit fraud. In order to improve fraud detection and prevention by considering a fourth component, Wolfe and Hermanson presented the Fraud Diamond theory in 2004.

2.5.1 Fraud Diamond Theory

In 2004, the fraud triangle was expanded to include the fraud diamond. According to this theory, even with the other three factors, an individual may still not commit fraud if there is no 'capability'. Capability pertains to an individual's traits and abilities, including the individual's position in the organization, intelligence, and the expertise required to commit fraud. According to the fraud diamond theory, four requirements must be met in order for fraud to occur: (a) an incentive, typically in the form of financial pressure; (b) an opportunity; (c) rationalization; and (d) capability

(Yendrawati et al., 2019). The inclusion of capability implied that fraud cannot happen unless the perpetrator possesses the necessary skills and abilities to perpetrate fraud, even when the other three elements are present (Paschoal et al., 2020). Fraud takes place when all four components of the fraud diamond theory are present. In this study, the fraud diamond developed by a study will be employed as a detection and prevention tool (Wolfe and Hermanson, 2004). Traits for committing fraud include (1) The individual's position in the organization; (2) the ability to recognize and take advantage of internal control weaknesses; (3) a strong sense of self-worth and confidence; (4) the ability to influence others to commit or conceal fraud, and; (5) the ability to lie effectively and consistently and handle stress well.

2.6 Fraud Detection and Prevention

Financial institutions' collective policies, procedures, protocols, and technologies to safeguard their assets, systems, and clients from fraud are referred to as bank fraud detection and prevention. Behavioral profiling, account monitoring, threat monitoring, and proactive risk identification are all included in detection. Proactive threat mitigation strategies including creating internal controls, training staff, and putting multi-layered security in place, are all part of prevention. (Wingard, 2023). Systematically identifying and evaluating fraud risks and proactively implementing preventative and investigative steps to reduce such risks are all part of fraud risk management. (Team Focal, 2024). Prevention involves procedures, guidelines, strategies, educating, and interaction to prevent fraud, while detection focuses on recognizing and preventing it. Prevention strategies are crucial, but not without risk. Awareness of fraud risk management and adequate detective controls are effective deterrents.

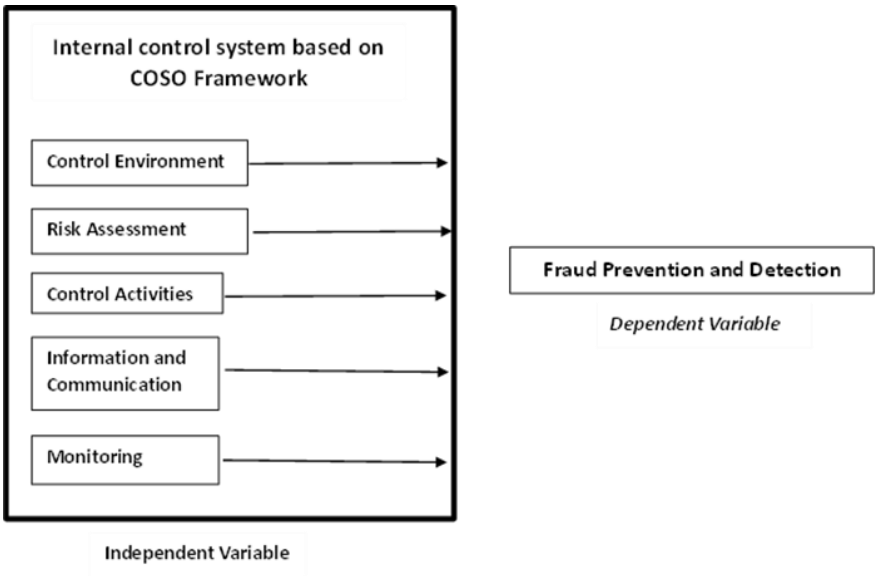
By showing that preventative controls are functioning as planned and by spotting fraud when it does happen, detective controls increase the efficacy of a fraud risk management program. Detective controls are not meant to stop fraud, even though they could show that it has happened or is happening. Although fraud can occur in any business, not all of them can be stopped, and doing so is not always cost-effective. A business may decide that designing its controls to detect certain fraud schemes rather than preventing them is more cost-effective. Both fraud detection and prevention must be taken into account by organizations.

According to a study, combining prevention and detection helps strengthen weaker businesses' defenses against fraud (Riney, 2018). A study supported the idea that prevention is the most cost-effective strategy for handling financial loss due to fraud (Sow et al., 2018). Hence, fraud prevention refers to an organization's practical steps to prevent or stop fraud (ACFE, 2020). The proactive goal of fraud prevention is to prevent fraudulent activity before it starts. It entails implementing policies, procedures, and systems designed to lessen the likelihood of fraud occurring within a company. This entails establishing internal controls and checks and balances, thoroughly screening vendors and workers, and implementing anti-fraud rules and procedures.

On the other hand, fraud detection is the process of discovering dishonest practices inside an organization. It focuses on identifying unlawful activity to allow for a prompt response and reduce damage. It ensures compliance and reduces the harm from possibly fraudulent behavior by using statistical models and machine learning to find doubtful patterns. This entails looking for anomalies and discrepancies in data, watching atypical transactions, and seeing any possible red flags or warning indicators linked to fraudulent behavior. (Chia, 2023). Therefore, fraud detection deters people from engaging in fraudulent conduct by raising the perceived danger of being caught (Jeppesen, 2019). Fraud detection plays a critical part in fraud investigation and prevention since the timeliness and method with which fraud is identified can significantly affect the severity of fraud, which may assist in curbing forthcoming scheme incidents (ACFE, 2020).

The Rural Bank Association of the Philippines (RBAP) also held fraud prevention seminars for its members with the assistance of the National Bureau of Investigation (NBI) and the Anti-Money Laundering Council (AMLC) to strengthen the industry's defenses against financial fraud or crime.

2.7 Conceptual Framework



Using the COSO framework to compare the current control environment to the five components can provide significant benefits for banks and other financial institutions. The framework provides banks with the data they need to make informed decisions at all levels of management, as well as more effective internal controls to mitigate risk. It can also assist firms improve their fraud risk management efficacy. Furthermore, the framework enables businesses to create controls that detect fraud early on, prevent it from occurring, and effectively handle fraud incidents when they do occur. (Vincent, 2023).

Fraud prevention and detection are the methods and processes that firms implement to limit the possibility of fraudulent conduct and identify instances of fraud when they occur. These programs seek to safeguard the organization's assets, reputation, and financial well-being by prohibiting fraudulent behavior and implementing measures to combat and reduce fraud threats. Avoiding fraud entails using proactive controls and safeguards to reduce the probability of acts of fraud. Preventing fraud in an organization requires fostering a culture of honesty, morality, and responsibility. This entails encouraging moral conduct, establishing precise guidelines, and cultivating a positive reporting atmosphere.

Distributing essential functions and responsibilities among different personnel helps to limit the risk of conspiracy, a scheme, and unlawful conduct. By guaranteeing that no single person has complete control over a process or transaction, the company decreases the possibility of fraud. The segregation of duties is all about preventing any one person from having complete control over any process. This spreads accountability throughout a team, making it more difficult for any one individual to purposefully or inadvertently evade a business procedure or standard. It also helps reduce risk in the event that someone with malicious intent does manage to infiltrate your systems or dupe an employee. (Dekker, 2023). Examples of internal controls measures that aid in fraud prevention are the authorization procedures, review and approval systems, and proper documentation.

These controls provide checks and balances to ensure that transactions are legitimate, comprehensive, and in accordance with policies and procedures. It is critical to recognize and evaluate potential fraud risks specific to the organization's operations. This allows the organization to set fraud prevention initiatives as a top priority and create focused controls to successfully handle the risks that have been identified. Effective fraud prevention and detection measures require a comprehensive and multi-faceted approach that incorporates preventive controls, continuous monitoring, employee awareness, and prompt response to potential fraud. By implementing robust fraud prevention and detection strategies, organizations can reduce the financial and reputational impact of fraud and preserve stakeholder trust.

The Fraud Risk Framework offers a thorough collection of key components and best practices to utilize as a roadmap when creating strategic, risk-based anti-fraud initiatives. (GAO, 2024). By consistently and deliberately reducing the probability and impact of fraud, fraud risk management aims to maintain program integrity. Having measures in place to stop, identify, and address fraud is only one aspect of strategic fraud risk management. Instead, it also includes organizational and environmental factors that influence or help managers achieve their goal of mitigating fraud risks. The Fraud Risk Framework divides best practices into four categories: commit, assess, design and implement, and evaluate and adapt. According to the US Government Accountability Office (GAO), the initial element of the fraud risk framework, dedicating to combating fraud can be accomplished by creating an internal environment and structure that promotes fraud risk management.

The third step in successfully managing fraud risks is design and implementation, which entails creating and carrying out a plan with particular control measures to lessen the evaluated fraud risks and working together to guarantee successful execution. The final step in GAO's Fraud Risk Framework is to assess results using a risk-based methodology and modify operations to strengthen fraud risk administration. On another note, COSO and ACFE also proposed a Fraud Risk Management Guide, which discusses the five fraud risk management principles that fully supported, completely aligned with, and paralleled by the COSO 2013 IC Framework's 17 internal control principles. The first fraud risk management principle states that the organization creates and disseminates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management, as well as their dedication to high integrity and ethical values regarding managing fraud risk.

This value aligns with COSO's control environment component which highlights the importance of the independence of the board of directors in overseeing the development and performance of internal control and the administration's pledge to honor value and moral principles. Meanwhile, the second principle of fraud risk management correlates with COSO's risk assessment component where the company counts the potential for fraud in measuring risks to the accomplishment of goals. The principle states that the business carries out inclusive fraud risk assessments to pinpoint definite fraud schemes and risks, evaluate their probability and implication, assess current fraud control activities, and execute activities to lessen residual fraud menaces.

The fraud mitigation concept summarizes the control activities component of the internal control structure. The premise asserts that the organization selects, develops, and implements preventative and proactive deception control operations to reduce the chance of a fraud incidence occurring or going unnoticed promptly. Additional fraud risk management principle complements the information and communication COSO component. The concept indicates that the business builds an

interface to receive details regarding probable fraud and performs a cohesive investigation and corrective action strategy to address fraud appropriately and swiftly. Finally, the 5th fraud risk prevention concept provides assistance for COSO's oversight component. The concept indicates that the company selects, develops, and conducts periodic reviews to establish whether each of the five fraud risk management principles is present and operational. This includes promptly communicating any flaws in the fraud risk management strategy to those who are accountable for corrective action, which includes the members of the board of directors and senior management.

3. Methods

The researcher employed a quantitative approach in reviewing the impact of the internal control system on detecting and preventing fraud. This study was conducted on 55 employees from different branches and corporate units. The population was comprised of the members of the board, senior management, officers, and rank-and-file personnel with tenures ranging from less than 5 years to more than 20 years.

4. Data Analysis

This section gives an analysis of the findings according to the (i) extent of implementation of internal control systems implementation in terms of (5) components of the COSO Framework to prevent and detect fraud, (ii) the level of agreement of the respondents on the relation between operational controls and the components of the Fraud Diamond in detecting and preventing fraud, (iii) the difference in assessed extent of internal control systems implementation of the respondents when grouped according to profile variables, and (iv) the difference in assessed level of agreement on the triggering factors for the occurrence of fraudulent activities.

4.1 Extent of Internal Control Systems implementation in terms of the components of the COSO framework

Table 1: Extent of Internal Control Systems Implementation in terms of Control Environment

	Mean	Interpretation
1. The members of the board oversees, governs, and guides senior management through regular board committee meetings.	3.85	Great Extent
2. The effectiveness of the internal control system is discussed with the management on a regular basis.	3.93	Great Extent
3. The management, internal auditors, and external auditors perform timely reviews of evaluations of internal controls.	3.89	Great Extent
4. Periodic efforts are made to ensure that management has appropriately followed up on recommendations and concerns expressed by auditors and supervisory authorities on internal control weaknesses.	3.85	Great Extent
5. Formation of an independent audit committee to support the board in fulfilling its duties. (Audit, Risk and Compliance Committee)	3.89	Great Extent
6. Propose/Amend pertinent fraud prevention corporate policies and manuals in a regular Management Meeting.	3.93	Great Extent
7. Senior management assigns those in charge of a particular unit's operations or duties the task of create more detailed internal control and procedures.	3.95	Great Extent
8. Ensure that the managers to whom they have delegated these tasks develop and carry out appropriate policies and procedures.	3.75	Great Extent

Table 1 (cont): Extent of Internal Control Systems Implementation in terms of Control Environment		
9. Ensure that activities are carried out by competent personnel who possess the requisite technical skills and expertise. Staff should receive fair pay and have regular training and skill updates.	3.15	Moderate Extent
10. Establish promotion and compensation policies that promote good behaviors.	2.95	Moderate Extent
11. Promotes strong ethical and integrity standards and establish an organizational culture that highlights and exemplifies the value of internal controls for all staff levels.	3.80	Great Extent
12. Dissemination and implementation of Fraud Reporting Policy.	3.82	Great Extent
13. Periodic review of the Disciplinary Committee Charter and Bank's Code of Conduct.	3.87	Great Extent
14. Bank personnel recognize their function in the internal controls procedure and are actively engaged in it.	3.82	Great Extent
15. All relevant personnel have access to well-written documentation of operational procedures.	3.78	Great Extent
16. Any operational issues, instances of infractions to the COC or other policy breaches or noted unlawful activities are reported to appropriate level of management.	3.84	Great Extent
Composite Mean	**3.75**	**Great Extent**

As shown in Table 1, the survey garnered a composite mean of 3.75 in terms of control environment. With this rating, it can be inferred that the respondents agreed that the Bank has established a strong foundation that promotes its commitment to integrity and ethical behavior, governance oversight, and effective internal control practices. In summary, areas where respondents agreed to a "great extent" include leadership involvement, effective communication of policies and procedures, and a commitment to ethical behavior and continuous improvement. On the other hand, areas such as staff qualifications and compensation alignment were at a "moderate extent" and could be further enhanced to strengthen the control environment even more.

Table 2: Extent of Internal Control Systems Implementation in relation to Risk Assessment (Risk recognition and Assessment)		
	Mean	**Interpretation**
1. Senior management determines and assesses the internal and external factors that may negatively impact the banking organization's ability to meet its operational, information and compliance goals. These include risks related to credit, market, liquidity and operational risk.	3.93	Great Extent
2. Identifies and takes into account both the internal factors (such as the bank's operations, personnel quality, organizational changes and employee turnover) and the external factors (such as fluctuating economic conditions, industry shifts, and technological advancements) that could negatively impact the achievement of the bank's objectives for effective risk assessment.	3.60	Great Extent
3. The risk assessment is carried out at the stage of specific businesses and across the wide spectrum of operations and subsidiaries of the consolidated banking organization.	3.93	Great Extent
4. Senior management ensure that the risks affecting the achievement of the bank's strategies and objectives are continuously assessed.	3.78	Great Extent
5. Internal controls are considered for revision to properly handle any new or previously uncontrolled risks.	3.93	Great Extent
6. Existence and implementation of Enterprise Risk Management (ERM) for assessment and improvement of business risk administration.	2.93	Moderate Extent
7. Simulation and regular updating of Business Continuity Plan (BCP)	2.80	Moderate Extent
8. Risk-based approach on Independent Compliance Testing (ICT), Regular or Surprise Audit Examination with assessment of its results. (Conducted by Internal Audit, Compliance, External Auditors and the BSP)	3.89	Great Extent
9. Employment of comprehensive risk and control self- assessments (RCSAs) on a bank wide basis	3.62	Great Extent
10. Identification and evaluation of the following across organization		
➢ inherent risk	3.75	Great Extent
➢ efficacy of the control environment	3.93	Great Extent
➢ residual risk	3.78	Great Extent
11. Establishment and evaluation of Risk Register	3.38	Great Extent
12. Defining action points and assigning to one or more responsible unit/s	3.91	Great Extent
Composite Mean	**3.65**	**Great Extent**

A composite mean of 3.65 was gathered in terms of risk assessment which indicates that the respondents agreed that the organization demonstrates comprehensive practices in identifying, evaluating, and managing risks across various dimensions, although specific areas such as ERM and BCP could benefit from further enhancement.

Table 3: Extent of Internal Control Systems Implementation in terms of Control Activities (Control Activities and Segregation of Duties)		
	Mean	**Interpretation**
1. Senior management establish an appropriate control structure to ensure effective internal controls, defining the control activities at		
➢ appropriate activity controls for various departments or divisions;	3.69	Great Extent
➢ physical controls;	3.80	Great Extent
➢ periodic review in accordance with exposure limits;	3.98	Great Extent
➢ a system of approvals and authorizations; and	3.96	Great Extent
➢ a system of authentication and balancing.	3.91	Great Extent
2. Fraud prevention efforts initiated by Human Resources Department prior and during employment/on boarding:		
➢ Background investigation	2.95	Moderate Extent
➢ Life style checking	3.07	Moderate Extent
➢ Regular performance evaluation	3.07	Moderate Extent
➢ Fair reward schemes	3.69	Great Extent
➢ Staff reporting policy	3.11	Moderate Extent
3. The workplace's distributive and procedural policies are fair.	3.65	Great Extent
4. Minimum Internal Control Measures		
➢ Regular Cash review / cash count	3.75	Great Extent
➢ Surprise Cash Count	3.82	Great Extent
➢ Independent Balancing	3.89	Great Extent
➢ Physical Handling of Transactions	3.95	Great Extent
➢ Joint Custody	3.96	Great Extent
➢ Dual Control	3.93	Great Extent
➢ Number control	3.98	Great Extent
➢ Confirmation of Accounts	3.93	Great Extent
➢ Cash Reconciliation	3.98	Great Extent
➢ Balance Confirmation (savings and loans)	3.93	Great Extent
5. Following functions are separated among employees:		
➢ Approval	3.95	Great Extent
➢ Accounting/reconciling	3.95	Great Extent
➢ Asset custody	3.95	Great Extent
6. Person who requisitions the purchase of bank supplies, furniture and fixture and other assets is not the individual who allows the purchase.	3.91	Great Extent
7. Person who approves the purchase of bank whether through cash or check should not be the person who reconciles the monthly financial reports.	3.96	Great Extent
8. The individual that manages and balances accounting data should not be granted administration of checks.	3.91	Great Extent
9. Person who opens the mail and prepares a listing of checks received should not be the person who makes the deposit.	3.95	Great Extent
10. The individual who examines mail and compiles a list of checks collected ought to not be the same person who keeps accounts receivable documents.	3.95	Great Extent
11. Regularizing fraud-related trainings to all personnel and level of management.	3.87	Great Extent
12. Use of passwords and monitoring of user access to system.	3.91	Great Extent
Composite Mean	**3.78**	**Great Extent**

As shown above, an overall mean score of 3.78 was gathered from the respondents in reference to control activities. This indicates that the bank has implemented activities designed to ensure effective internal controls, prevent fraud, maintain fairness in policies and procedures, and safeguard its assets. The respondents agreed that there was segregation of duties, minimum internal control measures, and fraud awareness through the provision of training. Fraud prevention efforts initiated by the Human Resource Department before or during employment could be further enhanced particularly in conducting background investigations, lifestyle checking, and regular performance evaluation which garnered a moderate extent according to the respondents.

Table 4: Extent of Internal Control Systems Implementation in terms of Information and Communication		
	Mean	**Interpretation**
1. Establish effective channels of communication to ensure that all staff are fully aware of policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.	3.58	Great Extent

Table 4 (cont): Extent of Internal Control Systems Implementation in terms of Information and Communication		
2. Encourage the complete flow of information throughout the organization – upward, downward and across the organization	3.65	Great Extent
3. Establishment and maintenance of management information systems that cover all of its activities and are accessible via both electronic and non-electronic channels.	3.71	Great Extent
4. Risks in the electronic information systems and the use of information technology are effectively controlled by the business through general and application controls in order to avoid disruptions to business and potential losses.	3.74	Great Extent
5. Cascading of the approved corporate policies and manuals in a regular Branch Manager / Area Head Meeting through issuance of internal memoranda and re-tooling.	3.84	Great Extent
6. Collaborative discussion of the cascaded policies, implementing rules and regulations between branch/department head and personnel.	3.85	Great Extent
7. Regularizing anti-fraud training programs focused on AMLA and other related fraud detection courses.	3.84	Great Extent
8. Launching hotlines	3.16	Moderate Extent
9. Secure and discrete whistleblowing policy and procedures.	3.36	Moderate Extent
10. Existence of adequate and comprehensive internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making.	3.95	Great Extent
Composite Mean	**3.67**	**Great Extent**

A composite mean of 3.67 about the information and communication component of the COSO Framework indicates that the respondents agreed that the bank effectively communicates information, manages risks related to information systems, enhances anti-fraud training programs, and ensures that relevant information reaches all stakeholders as needed. In summary, the bank shows a strong commitment through established practices such as internal control modifications, transaction authorizations, verification processes, asset management controls, and advanced security measures. Areas for potential enhancement include the available hotlines and ensuring a secure and discrete whistleblowing policy and procedures.

Table 5: Assessment on Internal Control Systems and Designs being used by the RB in terms of Monitoring Activities		
	Mean	**Interpretation**
1. Constant modification of internal control activities	3.67	Great Extent
2. Approval and permissions for specific transactions, such as refunds for expenses before payment.	3.96	Great Extent
3. Purchase requisition prior to procurement	3.96	Great Extent
4. Validation such as inspection of reports by a supervisor to ensure the truthfulness and precision of transactions performed by their employees.	3.84	Great Extent
5. Periodic asset counts and inventory	3.91	Great Extent
6. Confirming receivables and payables with relevant parties	3.91	Great Extent
7. Account reconciliation such as comparing the total cash balance with the combined individual cash accounts on hand and in banks Reconciling accounts by comparing the overall cash balance with the sum of individual cash accounts held both on-site and in banks.	3.91	Great Extent
8. Evaluating business performance by comparing actual revenue and/or expenses to budgeted figures.	3.85	Great Extent
9. Monitoring unit or department performance against objectives	3.93	Great Extent
10. Access management, including the use of passwords to limit entry to a computer or system.	3.93	Great Extent
11. Granting file access to authorized users or ensuring that individuals are held responsible for the custody of cash, supplies, or equipment.	3.78	Great Extent
12. Adoption of Fraud Prevention System Software and Design		
➢ Artificial intelligence (AI)	1.00	Least Extent
➢ Machine learning	2.00	Moderate Extent
➢ Biometric authentication	1.00	Least Extent
➢ Two-factor and/or multi-factor authentication	1.98	Moderate Extent
➢ Advanced analytics	1.00	Least Extent
➢ Multi-layered security systems	2.00	Moderate Extent
Composite Mean	**3.04**	**Moderate Extent**

A composite mean of 3.04 indicates moderate extent of monitoring activities within the bank. While many key controls are implemented to a great extent, the respondents identified adopting advanced technologies for fraud prevention as an area where improvements could be considered. The identified areas with the lowest mean in terms of fraud prevention system software and design implemented within the Bank are the utilization of AI, advanced analytics, and biometric authentication. To further enhance effectiveness, focusing on advanced security measures and continuous improvement in monitoring practices would be beneficial.

4.2 Level of Agreement of the Respondents on the relationship between internal control and the elements of the Fraud Diamond detecting and preventing schemes.

Table 6: Level of Agreement of the Respondents on the Relation between Internal Control and Pressure		
	Mean	**Interpretation**
1. Financial difficulty / un paid debts	4.69	Strongly Agree
2. Family Problem	4.58	Strongly Agree
3. Investment issues / conflict	4.62	Strongly Agree
4. Unfair reward schemes	4.73	Strongly Agree
5. Inconsistent audits / examination	4.51	Strongly Agree
6. Unavailability of fraud hotlines	4.65	Strongly Agree
7. Unsecure and vague whistleblowing policy	4.71	Strongly Agree
8. Absence of performance evaluation	4.80	Strongly Agree
9. Peer pressure for success	4.76	Strongly Agree
10. Excessive reliance to social validation resulting to living beyond means and uncontrollable expenses	4.67	Strongly Agree
Composite Mean	**4.67**	**Strongly Agree**

Overall, respondents strongly agreed that there is a significant link between internal control weaknesses and the components of the Fraud Diamond in fraud detection and prevention. In this study, the absence of performance evaluation, peer pressure for success, and unfair reward schemes were identified as the most likely examples of pressure that could motivate employees to commit occupational fraud. This result aligned with the findings highlighting the importance of strong internal controls including performance assessment, equitable reward programs, unannounced audits, confidential whistleblowing mechanisms., and monitoring to minimize fraud inducements (Abei, 2021).

Table 7: Level of Agreement of the Respondents on the Relation between Internal Control and Opportunity		
	Mean	**Interpretation**
1. Heavy reliance on manual operations	4.62	Strongly Agree
2. Poor supervision and monitoring	4.75	Strongly Agree
3. Improper documentation	4.55	Strongly Agree
4. Negligence of operational checking and review	4.78	Strongly Agree
5. Poor communication of specification of functions	4.73	Strongly Agree
6. Weak core banking systems update	4.58	Strongly Agree
7. Non performing cash reviews	4.71	Strongly Agree
8. Absence of fraud reporting policy	4.80	Strongly Agree
9. Lack of staff rotation policies	4.67	Strongly Agree
10. Non-modification of internal control procedures even if necessary	4.80	Strongly Agree
11. Poor "tone at the top," indicating a lack of commitment to ethics, honesty, and integrity from upper management and the board of directors.	4.65	Strongly Agree
12. Poor employee recruitment practices	4.85	Strongly Agree
13. Absence of check and balance system	4.60	Strongly Agree
Composite Mean	**4.70**	**Strongly Agree**

This study confirmed the findings from previous research that fraud chance stems from outdated internal control systems (Nawawi and Salin, 2018; Abei, 2021). Additionally, the research determined poor employee onboarding processes and the absence of fraud reporting policy as the areas which could highly influence fraud opportunity within the Bank. The uniformly high mean scores across all items indicate a robust consensus among the respondents on the importance of robust internal controls in mitigating the risk of fraud. Since fraud opportunities arise from weaknesses in internal systems, it is essential to establish policies that facilitate regular updates to the organization's internal controls. Furthermore, to strengthen the implemented internal control system, resources should be allocated for conducting background investigations of interested applicants before onboarding and establishing a clear guideline for reporting incidents of fraud.

Table 8: Level of Agreement of the Respondents on the Relation between Internal Control and Rationalization		
	Mean	**Interpretation**
1. Experiencing unfair treatment can lead to feelings of resentment towards their manager or employer, causing individuals to believe that committing fraud is a means of seeking revenge.	4.53	Strongly Agree
2. Weak moral managerial culture and establishing unfair tasks for staff.	4.62	Strongly Agree
3. A negative tone at the top causes individuals to emulate the behavior of those in higher positions within the corporate hierarchy.	4.64	Strongly Agree
4. A mindset of "There is no other solution" can lead an employee to believe that they risk losing everything (such as their job) unless they resort to committing fraud.	4.56	Strongly Agree
5. Inadequate training related to function before actual deployment.	4.60	Strongly Agree
6. Poor dissemination of approved policies of bank.	4.76	Strongly Agree
7. Lack of orientation on personnel related to bank policies, rules and regulations.	4.71	Strongly Agree
8. Having “other employees are wasting money all over the place” mindset.	4.75	Strongly Agree

Table 8 (cont): Level of Agreement of the Respondents on the Relation between Internal Control and Rationalization		
9. Self-justification of being under paid and unfair remuneration policy.	4.71	Strongly Agree
10. Consuming "I'm only borrowing the money" outlook	4.75	Strongly Agree
Composite Mean	**4.66**	**Strongly Agree**

The respondents strongly agreed that poor dissemination of approved policies affects the likelihood of fraud. The study also determined that employees who might commit fraud have a mindset that they are only temporarily borrowing money from the Bank or that other employees are wasting money. Generally, the Bank must set up programs that support moral education and foster robust corporate principles. This will foster the development and maintenance of strong moral standards, positive values, and cohesive staff behavior.

Table 9: Level of Agreement of the Respondents on the Relation between Internal Control and Capability		
	Mean	**Interpretation**
1. Access Sharing	4.71	Strongly Agree
2. Heavy reliance on field collection of payment and solicitation of savings.	4.51	Strongly Agree
3. Poor supervision and checking	4.76	Strongly Agree
4. Absence of exercising dual control and joint custody	4.71	Strongly Agree
5. Weak implementation of segregation of duties	4.73	Strongly Agree
6. Non-review of approving limits and signing authority policy for possible deviations	4.56	Strongly Agree
7. Absence of job rotations	4.75	Strongly Agree
8. Unstable operational banking system due to sudden fortuitous events.	4.76	Strongly Agree
9. Undetected conflict of interest occurred in related parties.	4.64	Strongly Agree
10. Undisclosed related party transactions.	4.71	Strongly Agree
Composite Mean	**4.68**	**Strongly Agree**

The respondents strongly agreed on all the items related to fraud capability, as shown in Table 4.4. Among these items, the weaknesses that most respondents agreed with are poor supervision and checking, unstable operational banking system due to sudden fortuitous events, and absence of job rotations. Concerning previous research of the findings of this study affirm the importance of segregation of duties and job rotation in reducing the likelihood of fraud in an organization (Shonhadji and Maulidi, 2020; Abei, 2021).

4.3 Differences in the Assessed Extent of Internal Control Systems Implementation when Convened according to Profile Variables

Table 10: Differences in the Assessed Extent of Internal Control Systems Implementation when Grouped according to Position						
Variable	**Age**	**Mean**	**F-value**	**p- value**	**Decision on Ho**	**Interpretation**
Control Environment	Board of Directors	3.98	3.561	.005	Reject	Significant
	Senior Management	3.98				
	Independent Unit	3.73				
	Branch Personnel	3.75				
	Corporate Unit Personnel	3.75				
	Department/Corporate Unit Head	3.81				
	Branch Personnel	3.69				
Risk Assessment	Board of Directors	4.00	10.974	<.001	Reject	Significant
	Senior Management	4.00				
	Independent Unit	3.49				
	Branch Personnel	3.51				
	Corporate Unit Personnel	3.64				
	Department/Corporate Unit Head	3.81				
	Branch Personnel	3.74				
Control Activities	Board of Directors	3.85	8.630	<.001	Reject	Significant
	Senior Management	3.84				
	Independent Unit	3.65				
	Branch Personnel	3.80				
	Corporate Unit Personnel	3.87				
	Department/Corporate Unit Head	3.85				
	Branch Personnel	3.84				

Table 10 (cont): Differences in the Assessed Extent of Internal Control Systems Implementation when Grouped according to Position						
Information and Communication	Branch Personnel	3.78	5.240	<.001	Reject	Significant
	Board of Directors	3.97				
	Senior Management	3.80				
	Independent Unit	3.57				
	Branch Personnel	3.85				
	Corporate Unit Personnel	3.73				
	Department/Corporate Unit Head	3.77				
Monitoring Activities	Branch Personnel	3.54	4.279	.002	Reject	Significant
	Board of Directors	3.06				
	Senior Management	3.12				
	Independent Unit	2.90				
	Branch Personnel	3.09				
	Corporate Unit Personnel	3.09				
	Department/Corporate Unit Head	3.12				
Overall	Branch Personnel	3.08	7.237	<.001	Reject	Significant
	Board of Directors	3.77				
	Senior Management	3.75				
	Independent Unit	3.47				
	Branch Personnel	3.60				
	Corporate Unit Personnel	3.61				
	Department/Corporate Unit Head	3.67				

It was clearly shown from the table that there is a significant difference in the assessed extent of internal control systems implementation in terms of components of the COSO framework. when grouped according to position as indicated by p-values of at most .005. Such p-values are less than the .05 level of significance that led to reject the null hypothesis. For the control environment, the result garnered agreement to a great extent across all respondents. The members of the board and senior management equally gave their highest mean rating of 3.98 while the Independent Unit obtained the lowest mean of 3.73. This result supports the COSO Framework which emphasizes the function of the body and senior in designing and executing mechanisms. The result indicates that the BOD and Senior Management perceive the bank's control environment more favourably while the independent unit personnel perceive them less.

As to risk assessment, all respondents agree to a great extent on the effectiveness of the bank's risk assessment. The members of the board and senior management gave the highest rating of 4.00 while the Independent Unit gave the lowest mean score of 3.49. The difference in perception can be attributed to several factors such as access to information, different experiences, feedback and reporting mechanisms, and risk tolerance. For control activities, the corporate unit personnel gave the highest rating of 3.87 while the independent unit gave the lowest rating of 3.65 which can be attributed to the difference in implementation and design as perceived by the process owners and the independent unit, the operational challenges, and gaps to operations. For information and communication, the survey garnered the highest mean of 3.97 from the board of directors while the lowest mean was from the independent units who gave 3.57. Regarding the bank's monitoring activities, the majority of the respondents only moderately agreed where the garnered rating ranged from 2.90 to 3.54.

In general, the assessment of the respondents on the internal control systems implementation when grouped according to position was based on a p-value of 7.237. Such p-value is less than .05 level of significance led to reject the null hypothesis. This indicates that the different position groups of respondents have different insights on the internal control systems implementation. Overall, the members of the board gave the highest rating for the internal control measures followed by the Senior Management indicating their agreement to a great extent with the Bank's implementation of operational control measures while the Independent Unit and the branch personnel agreement ranged from moderate to great extent.

Table 11: Differences on the Assessed Extent of Internal Control Systems Implementation when Grouped according to Number of Years in Bank

Variable	Years in Bank	Mean	F-value	p- value	Decision on Ho	Interpretation
Control Environment	less than 5 years	3.74	1.721	.160	Failed to Reject	Not Significant
	5 to 10 years	3.81				
	11 to 15 years	3.56				
	16 to 20 years	3.67				
	more than 20 years	3.69				
Risk Assessment	less than 5 years	3.59	1.513	.213	Failed to Reject	Not Significant
	5 to 10 years	3.73				
	11 to 15 years	3.86				
	16 to 20 years	3.63				
	more than 20 years	3.71				
Control Activities	less than 5 years	3.76	.518	.723	Failed to Reject	Not Significant
	5 to 10 years	3.79				
	11 to 15 years	3.84				
	16 to 20 years	3.84				
	more than 20 years	3.81				

Table 11 (cont): Differences on the Assessed Extent of Internal Control Systems Implementation when Grouped according to Number of Years in Bank						
Information and Communication	less than 5 years	3.68	2.458	.057	Failed to Reject	Not Significant
	5 to 10 years	3.73				
	11 to 15 years	3.40				
	16 to 20 years	3.43				
	more than 20 years	3.53				
Monitoring Activities	less than 5 years	3.02	.573	.684	Failed to Reject	Not Significant
	5 to 10 years	3.06				
	11 to 15 years	3.00				
	16 to 20 years	3.02				
	more than 20 years	3.12				
Overall	less than 5 years	3.56	1.216	.316	Failed to Reject	Not Significant
	5 to 10 years	3.63				
	11 to 15 years	3.53				
	16 to 20 years	3.52				
	more than 20 years	3.57				

Results showed that when categorized according to years in the bank, there is no discernible difference in the assessed extent of internal control systems implementation in terms of components of COSO framework as indicated by p-values ranging from.057 to .723. Such p-values are greater than .05 level of significance that failed to reject the null hypothesis. This may indicate that they have comparable assessments on the extent of internal control systems implementation.

4.4 Differences in the Assessed Level of Agreement of the Respondents on the relation between internal control and the components of the Fraud Diamond in detecting and preventing fraud when grouped according to Profile Variables

Table 12: Differences in the Assessed Level of Agreement of the Respondents on the relation between internal control and the components of the Fraud Diamond in detecting and preventing fraud when grouped according to Position						
Variable	**Position**	**Mean**	**F-value**	**p- value**	**Decision on Ho**	**Interpretation**
Internal Control and Pressure	Board of Directors	4.97	4.183	.002	Reject	Significant
	Senior Management	4.73				
	Independent Unit	4.37				
	Branch Personnel	4.77				
	Corporate Unit Personnel	4.73				
	Department/Corporate Unit Head	4.80				
	Branch Personnel	4.79				
Internal Control and Opportunity	Board of Directors	4.87	6.867	<.001	Reject	Significant
	Senior Management	4.69				
	Independent Unit	4.38				
	Branch Personnel	4.72				
	Corporate Unit Personnel	4.77				
	Department/Corporate Unit Head	4.84				
	Branch Personnel	4.90				
Internal Control and Rationalization	Board of Directors	4.83	5.572	<.001	Reject	Significant
	Senior Management	4.77				
	Independent Unit	4.37				
	Branch Personnel	4.60				
	Corporate Unit Personnel	4.53				
	Department/Corporate Unit Head	4.77				
	Branch Personnel	4.92				
Internal Control and Capability	Board of Directors	4.77	3.873	.003	Reject	Significant
	Senior Management	4.77				
	Independent Unit	4.45				
	Branch Personnel	4.64				
	Corporate Unit Personnel	4.55				
	Department/Corporate Unit Head	4.60				
	Branch Personnel	4.93				

Table 12 (cont): Differences in the Assessed Level of Agreement of the Respondents on the relation between internal control and the components of the Fraud Diamond in detecting and preventing fraud when grouped according to Position						
Overall	Board of Directors	4.86	6.887	<.001	Reject	Significant
	Senior Management	4.74				
	Independent Unit	4.39				
	Branch Personnel	4.68				
	Corporate Unit Personnel	4.64				
	Department/Corporate Unit Head	4.75				
	Branch Personnel	4.89				

Table 13: Differences on the Assessed Level of Agreement of the Respondents on the relation between internal control and the components of the Fraud Diamond in detecting and preventing fraud when grouped according to Years in Bank

Variable	Years In Bank	Mean	F-value	p- value	Decision on Ho	Interpretation
Internal Control and Pressure	less than 5 years	4.60	1.257	.299	Failed to Reject	Not Significant
	5 to 10 years	4.69				
	11 to 15 years	4.90				
	16 to 20 years	4.93				
	more than 20 years	4.83				
Internal Control and Opportunity	less than 5 years	4.58	2.505	.054	Failed to Reject	Not Significant
	5 to 10 years	4.78				
	11 to 15 years	5.00				
	16 to 20 years	4.94				
	more than 20 years	4.82				
Internal Control and Rationalization	less than 5 years	4.54	2.120	.092	Failed to Reject	Not Significant
	5 to 10 years	4.77				
	11 to 15 years	4.90				
	16 to 20 years	4.93				
	more than 20 years	4.67				
Internal Control and Capability	less than 5 years	4.58	2.065	.099	Failed to Reject	Not Significant
	5 to 10 years	4.75				
	11 to 15 years	5.00				
	16 to 20 years	5.00				
	more than 20 years	4.67				
Overall	less than 5 years	4.57	2.527	.052	Failed to Reject	Not Significant
	5 to 10 years	4.75				
	11 to 15 years	4.95				
	16 to 20 years	4.95				
	more than 20 years	4.75				

It can be gleaned from the table that the respondents differ significantly in their level of agreement on the relation concerning internal control and the components of the Fraud Diamond in terms of pressure, opportunity, rationalization, and capability when grouped according to position as indicated by p-values of at most .003 and a p-value which is less than .05 level of significance in terms of overall agreement These led to the rejection of the null hypothesis.

While there is a consensus among the respondents that internal control is crucial in addressing pressure, there is a significant difference in the level of agreement among different positions regarding the relation between internal control and the components of the theory. The members of the board and senior management generally showed the strongest belief in the significance of internal controls in mitigating the four components of fraud, while the Independent Unit perceived these links as weaker. These differences could stem from varying levels of exposure to and involvement in the design and execution of internal controls, access to information, experience and training, and exposure to control failures.

As shown from the table above, there is no significant difference in the level of agreement of the respondents on the relation between internal control and the components of the theory in detecting and preventing schemes in terms of pressure, opportunity, rationalization, and capability when grouped according to years in bank me as indicated by p-values ranging from. 054 to .299. Such p-values are greater than .05 level of significance that led to the nonrejection of the null hypothesis. With regards to the overall assessment of the level of agreement of the respondents, the relation between internal control and the components of the theory in detecting and preventing schemes is not significantly different as the obtained p-value is .053. Such p-value is greater than .05 level of significance that failed to reject the null hypothesis.

5. Conclusion

This study uncovers that internal control systems significantly affect fraud detection and prevention. Implementing internal control systems helps mitigate the triggering factors of fraud, such as incentive, opportunity, rationalization, and capability. The institution's various strong points regarding internal control systems are the effective communication of policies, commitment to ethical behavior, segregation of duties, implemented internal control measures, and fraud awareness training. This study also identifies areas of internal control systems for further enhancements of the institution particularly the utilization of advanced technologies to enhance the fraud prevention mechanism and combat new probable fraud schemes.

REFERENCES

Abei, Y., 2021. Impact of Internal Control on Fraud Detection and Prevention in Microfinance Institutions, Pp. 25-26 - 48-52

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

American Institute of Certified Public Accountants [AICPA], 2018. Welcome to Internal Control, https://www.aicpa-cima.com/resources/article/welcome-to-internal-control

American Institute of Certified Public Accountants [AICPA], 2020. Compliance Supplement Part 6, Pp. 3.

Ashfaq, K., and Rui, Z., 2019. The effect of board and audit committee effectiveness on internal control disclosure under different regulatory environments in South Asia. Journal of Financial Reporting and Accounting, 17 (2), Pp. 170-20 https://doi.org/10.1108/JFRA-09-2017-0086

Association of Certified Fraud Examiners (ACFE), 2024. Occupational Fraud 2024: A Report to the Nations, Pp. 7.

Cordero, T., 2024. GMA Integrated News, BSP's consumer protection through redress mechanism for online payments, https://www.gmanetwork.com/news/money/personalfinance/909400/explainer-bsp-s-consumer-protection-through- redress-mechanism-for-online-payments/story

COSO/ACFE, 2023. Fraud Risk Management Guide Executive Summary, Second Edition, Pp. 13.

Creswell J.W., and Guetterman, T.C., 2019. https://www.academia.edu/97363666/Quantitative_Research_Method.

Ilyas, S., Sutisna, D., and Saudi, M.H., 2021. The Role of Control Environment in Developing Internal Control Effectiveness and Good Corporate Government.

Jeppesen, K.K., The role of auditing in the fight against corruption. Journal of The British Accounting Review, 51 (5), Pp. 100798. https://doi.org/10.1016/j.bar.2018.06.001

Kabuye, F., Kato, J., Akugizibwe, I., and Bugambiro, N., 2019. Internal Control Systems, Working Capital Management and Financial Performance of Supermarkets, Cogent Business and Management, Pp. 4

Le, N.T.B., Vu, L.T.P., and Nguyen, T.V., 2020. The use of internal control systems and codes of conduct as anti-corruption practices: evidence from Vietnamese firms", Baltic Journal of Management, Vol. ahead-of-print No. ahead-of-print., https://doi.org/10.1108/BJM-09-2020-0338

Le, T.T.H., and Tran, M.D., 2018. The effect of internal control on asset misappropriation: The case of Vietnam. Journal of Business and Economic Horizons, 14 (4), Pp. 941-953. http://dx.doi.org/10.15208/beh.2018.64

Nawawi, A., and Salin, P.A.S.A., 2018. Internal Control and Employees' Occupational Fraud on Expenditure Claims, Journal of Financial Crime, 25 (3), Pp. 891-906.

Nugraha and Bayunitri, 2020. The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City).

Ordinario, C., 2024. Business Mirror, BSP and PDIC join forces against financial fraud, https://businessmirror.com.ph/2024/02/22/bsp-pdic-to-share-info-in-fighting-fraud-scam

Paschoal, A.L.P., de Araújo, Santos, N., and Faroni, W., 2020. The fraud diamond: Empirical evidence in the external demand reports of the Ministry of Transparency and General Comptroller of the Union (CGU) of Brazilian municipalities. Accounting Environment Journal - Federal University of Rio Grande do Norte-ISSN 2176-9036, 12(2), 136-156], 2020, https://doi.org/10.21680/2176-9036.2020v12n2ID18732

PhilStar Global, 2022. BSP slaps sanctions on BDO, UnionBank over massive online fraud, 2022, https://www.philstar.com/business/2022/04/28/2177432

Posey, B., COSO Framework definition, 2021, https://www.techtarget.com/searchcio/definition/COSO-Framework

PricewaterhouseCoopers (PwC), 2020. Global Economic Crime and Fraud Survey: The Philippine Report, Pp. 4, 13.

Riney, F.A., 2018. Two-Step Fraud Defense System: Prevention and Detection. Journal of Corporate Accounting and Finance, 29 (2), Pp. 74-86. https://doi.org/10.1002/jcaf.22336

Shonhadji, N., and Maulidi, A., 2020. Is it Suitable for your Local

Governments? Journal of Financial Crime, 2020

Sow, A.N.G., Basiruddin, R., Mohammad, J., and Rasid, S.Z.A., Fraud prevention in Malaysian small and medium enterprises (SMEs). Journal of Financial Crime, 25 (2), Pp. 499-517. https://doi.org/10.1108/JFC-05-20170049

Ta-asan, K., 2024. Business World, Anti-financial account scamming bill to help address threats — BSP, https://www.bworldonline.com/editors-picks/2024/01/23/570375/anti-financial-account-scamming-bill-to-help-address- threats-bsp

Team Focal, 2024. An In-depth Analysis of Fraud Risk Management in 2024, 2024, https://www.getfocal.ai/blog/fraud-risk- management

United States Government Accountability Office, 2024. Report to Congressional Committees Fraud Risk Management, Pp. 13-15.

Vincent, D., 2023. 7 Proven Benefits of The COSO Control Framework, https://pathlock.com/learn/7-proven-benefits-of- the-coso-framework/

Wingard, L., 2023. Fraud Management in Banking: Detection, Prevention and More, 2023, https://global.hitachi- solutions.com/blog/fraud-prevention-in-banks/

Yendrawati, R., Aulia, H., and Prabowo, H.Y., 2019. Detecting the likelihood of fraudulent financial reporting: An Analysis of fraud diamond. Asia-Pacific Management Accounting Journal, 14 (1), Pp. 43–69, https://doi.org/10.24191/apmaj.v14i1- 03