Perceptions of Risk Management and Bank Fraud Prevention in Ethiopian Banks: Employees' Perspective

Haile Anteneh[1*] Dhiraj Sharma[2]

1. Research Scholar at School of Management Studies, Punjabi University Patiala, Punjabi, India
2. Assistant Professor at School of Management Studies, Punjabi University Patiala, Punjabi, India

* E-mail of the corresponding author: hanteneh23@gmail.com

Abstract

Effective bank fraud prevention and management is crucial for financial institutions to mitigate risks and protect their assets. This study explores how employee perceptions of risk management practices relate to their perception of the bank's effectiveness in preventing fraud. An ordered probit model was used to analyze survey data collected from 475 employees across 17 Ethiopian private and public banks. The analysis revealed significant positive relationships between several bank practices and perceived fraud prevention effectiveness. Employees who perceived more robust risk management, control measures, training programs, technology use, and incident response protocols were more likely to believe the bank effectively prevented fraud. These findings highlight the importance of specific bank practices in fostering a positive employee perception of fraud prevention. Banks can leverage this knowledge to develop targeted strategies for strengthening areas with the strongest positive associations with perceived effectiveness. These can lead to improved employee awareness, better use of technology for fraud detection, and, ultimately, a more secure banking environment.

Keywords: Bank Fraud Prevention; Employee Perceptions; Ordered Probit Model; Risk Management; Control Measures; Training; Technology, Incident Response

DOI: 10.7176/RJFA/15-7-05

Publication date: July 30th 2024

1. Introduction

Bank fraud, a menacing threat to the financial sector, not only jeopardizes the stability and integrity of bank institutions (Hussaini *et al*., 2018) but also undermines the trust of customers and investors. Banks have a multi-layered defense plan to counter these dangers. According to Rohmatin *et al*. (2021), this approach combines strong governance and risk management procedures to promote ethical behavior and improve compliance monitoring. Furthermore, comprehensive policies and control mechanisms, employee education, and awareness campaigns combine to discourage fraud attempts and provide employees with the tools they need to get involved in prevention initiatives (Flowerastia *et al*., 2021; Musyoki, 2023).

In addition, banks are leading the way in utilizing data analytics and cutting-edge technology to keep ahead of constantly changing scams. Machine learning, artificial intelligence, and big data analytics make possible the detection of complex patterns suggestive of fraudulent activity and the identification of new trends (Byrapu *et al*., 2024; Olubusola *et al*., 2024). These improvements and efficient incident response procedures create a complete strategy to prevent fraud (Tariq *et al*., 2024).

Risk management and governance, control measures and policies, training and awareness, technology and analytics, and incident response and controls are essential elements that should be well executed in every organization's effort to attain its established objectives. This study used all these factors to measure bank fraud prevention capability. It prepared a questionnaire for bank employees and analyzed their responses using the ordered probit regression model. The study aimed to provide valuable insights into best practices for banks' fraud prevention strategies by exploring the efficacy of these strategies in preventing bank fraud, focusing on risk management and governance, control measures and policies, training and awareness, technology and analytics, and incident response and controls. By comprehending and implementing these strategies, banks can enhance their security posture, strengthen their resilience against fraudulent activities, and contribute to a reduction in bank fraud incidents.

2. Hypothesis Development

2.1 Risk Management and Governance (RMG)

Risk management and governance involve systematic processes to identify, assess, and mitigate organizational risks, particularly in financial institutions like banks. Strong risk management and governance procedures greatly lower the fraud rate in banks by boosting compliance monitoring, developing a culture of ethical behavior, and strengthening internal control efficacy. These, in turn, help create a banking environment that is safer and more resilient, which eventually boosts corporate governance and improves financial performance. Rohmatin *et al*. (2021) assert that by establishing strong internal controls and encouraging a culture of ethical behavior, effective governance and risk management techniques can greatly decrease the likelihood of fraud occurring. According to Hussaini *et al*. (2018), stronger fraud risk management procedures and a long-standing culture of risk-taking lead to safer banking and may even boost profits. Rehman and Hashim (2020) point out that banks can improve their corporate governance and control environment by using effective fraud prevention strategies. Ngigi *et al*. (2020) emphasize that effective risk assessment methods and appropriate governance monitoring form a solid basis for detecting and preventing fraud within banks. A more secure and resilient financial system can be achieved through proactive risk management of fraud by banks using a well-integrated Governance, Risk, and Compliance (GRC) approach, according to Knechel and Willekens (2006). Finally, according to Drogalas *et al*. (2017), a bank's capacity to detect, prevent, and investigate fraudulent actions can be greatly enhanced by a strong internal audit function backed by efficient governance systems.

H_1: *Stronger risk management practices and effective corporate governance will lead to a lower incidence of bank fraud.*

2.2 Control Measures and Policies (CMP)

Control Measures and Policies are protocols and procedures designed to prevent, detect, and respond to fraudulent activities. Banks that incorporate advanced technologies such as big data analytics and behavioral analytics, develop well-defined policies and procedures, and implement robust internal controls will experience a substantial decrease in fraud incidents. This results from a more comprehensive approach to identifying and averting fraudulent activities, improved threat intelligence, and enhanced detection capabilities. Musyoki (2023) asserts that internal solid controls are a powerful obstacle to fraudulent actions. He stresses the significance of clearly defined policies and procedures, division of responsibilities, and routine audits. According to Rahman and Anwar (2014), a well-designed combination of rules and control systems, backed by continuous monitoring and staff training, is essential to avoid bank fraud. As Philip et al. (2024) pointed out, big data analytics can improve control methods and regulations. A stronger defense against bank fraud can be achieved by combining thorough rules with strong internal controls (Rashid, 2022). According to Olaniyan *et al*. (2023), banks can boost their control measures and policies by combining threat intelligence with behavioral analytics. This gives them a better picture of the danger landscape and helps them spot suspicious conduct that could be hard to detect using traditional approaches.

H_2: *Implementing comprehensive control measures and effective fraud prevention policies will lower the incidence of bank fraud.*

2.3 Training and Awareness (TRA)

Training and awareness programs inform employees about fraud risks and prevention strategies. A more proactive and robust fraud prevention framework within banks results from comprehensive and continuous employee education programs that incorporate general awareness training, role-specific skills, behavioral science principles, and financial literacy elements. This enhancement in employees' ability to detect and prevent fraud is significant. According to Flowerastia *et al*. (2021), a stronger foundation for preventing fraud can be achieved by well-designed training and awareness programs that help employees spot suspicious activities. Regular and multi-channel delivery of effective security awareness campaigns is critical in shaping employee behavior and, according to Li *et al*. (2016), contributes to effective fraud prevention. For banks to keep up with the ever-changing fraud risks and keep their defenses strong, Abubakar (2024) stresses the need for a dynamic and dynamic training strategy focused on continuous learning and adaptation. Security awareness training programs can enhance their ability to influence employee conduct and decrease the risk of bank fraud by integrating behavioral science principles, according to Williams *et al*. (2019). Security awareness training, according to Magioli Sereno and Ang (2024), is critical for changing the mindset of employees and encouraging them to take the initiative to prevent fraud. Last but not least, Asker and Tamtam (2020) point out that training programs that include financial literacy enable staff to take a more active role in preventing fraud and providing better customer service.

H$_3$*: Increased employee training and awareness programs regarding fraud prevention will lead to a lower incidence of bank fraud.*

2.4 Technology and Analytics (TEA)

Technology and analytics encompass the application of cutting-edge resources such as artificial intelligence, data analytics, machine learning, and social network analysis. Using cutting-edge technology like machine learning, artificial intelligence, data analytics, and social network analysis improves banks' capacity to detect and prevent fraud. Because of these, a more secure financial environment is achieved through improved accuracy in recognizing fraudulent actions, detecting growing fraud patterns, and successfully resisting fraudulent schemes. In their study, Byrapu *et al.* (2024) compare machine learning to traditional rule-based systems and find that it can improve fraud detection accuracy. In their discussion, Philip *et al*. (2024) highlight how banks might uncover new fraud tendencies and create better detection models by examining massive and intricate datasets. Social network analysis can enhance the efficacy of fraud prevention techniques, as Chau and Faloutsos (2018) showed. By analyzing data from previously detected fraudulent credit card transactions, Ashraf *et al.* (2022) are able to detect fraudulent transactions. By showcasing AI's ability to detect anomalies within large and ever-changing datasets, Olubusola *et al*. (2024) prove that AI is superior at detecting complex patterns that indicate fraudulent conduct. The review explains the practical uses of AI in fraud detection by highlighting real-life examples of the technology's effectiveness in foiling scams.

H$_4$*: Using advanced technology and data analytics will lead to a more effective detection and prevention of bank fraud.*

2.5 Incident Response and Controls (IRC)

Incident Response and Controls are procedures that are designed to respond to fraudulent incidents in a timely and effective manner. The financial losses and reputational damage resulting from bank fraud incidents are substantially reduced by clear incident response plans based on thorough investigations and continuous improvement. Regular exercises improve employee readiness, bolstering the bank's defense against fraud, while data-driven insights refine fraud prevention strategies. The importance of incident response plans is emphasized by Tariq *et al.* (2024), who highlight the importance of effective investigation procedures, communication protocols, and defined roles. The efficacy of such plans is underscored by Samuel *et al*. (2023), who emphasize the importance of continuous refinement and comprehensive investigations. Ramadhan (2020) underscores the importance of root cause analysis in identifying vulnerabilities and implementing corrective actions. Achary and Shelke (2023) investigate the potential of data analytics to improve fraud detection models. Omar *et al*. (2016) indicate the significance of incident response exercises in improving employee preparedness for fraud.

H$_5$: The effectiveness of incident response and controls directly influences bank fraud prevention efforts.

3. Materials and Methods

3.1 Research and Instrument Design

This cross-sectional study employed a quantitative structured survey, drawing on positivist epistemology and realist ontology. A self-administered questionnaire was developed to measure assessment instruments, utilizing a five-point Likert scale ("strongly agree" to "strongly disagree"). To ensure content validity, the questionnaire underwent a two-step process. Firstly, it was reviewed by a diverse group of risk management experts from private banks, public banks, and central bank (6 in total). Secondly, a pilot test with 35 participants assessed the questionnaire's clarity, understandability, and language neutrality. Subsequent expert and participant feedback led to minor adjustments, ensuring that the final instrument effectively captured the intended measurements. Carefully designed sampling instruments were employed to encompass perspectives from various levels of the organizational hierarchy, resulting in a sample size of 537, which included top management, middle management, frontline staff, and back-office staff. Due to non-respondents and the identical answer (straightening), 475 replies were analyzed, producing a 90% response rate.

3.2 Preliminary Analyses

The study comprises 324 males (68.2%) and 151 females (31.8%). 28.2% are aged 21-30, 40.4% are 31-40, 28.8% are 40-50, and 2.5% are over 50. Regarding job positions, 8.0% are in top management, 16.8% in middle management, 26.1% are back-office staff, and 49.1% are frontline staff. Regarding experience, 21.9% have 0-5 years, 31.2% have 6-10 years, 29.9% have 11-15 years, and 17.1% have over 15 years of experience. Lastly, 33.5% work in public banks, while 66.5% are in private banks.

Descriptive statistics for the study's variables are presented in Table 1. Cronbach's Alpha was employed to assess the internal reliability of each instrument, with values exceeding 0.7 indicative of acceptable internal consistency (Taber, 2018). The overall Cronbach's Alpha for the study was 0.90. Individual instrument reliabilities ranged from 0.811 (RMG) to 0.876 (TRA), demonstrating reasonably good internal consistency for all measures.

Table 1. Descriptive Statistics and Cronbach's Alpha

Variables	**Mean**	**Std. Deviation**	**Cronbach's α**
Risk Management and Governance (RMG)	3.784	0.618	0.811
Training and Awareness (TRA)	4.079	0.659	0.876
Incident Response and Controls (IRC)	3.917	0.576	0.833
Technology and Analytics (TEA)	3.745	0.601	0.844
Control Measures and Policies (CMP)	3.876	0.646	0.842

Source: Authors (2024)

The suitability of exploratory factor analysis (EFA) for this study was assessed prior to factor extraction and hypothesis testing. Data suitability is typically evaluated using the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity. KMO values exceeding 0.8 indicate adequate sampling, while a statistically significant Bartlett's Test ($p < 0.05$) suggests that the data exhibits the absence of sphericity, a requirement for EFA (Shrestha, 2021). In this study, the KMO value was 0.899, and Bartlett's Test of Sphericity yielded a significance level of $p < .001$. These results confirm the data's appropriateness for further factor analysis.

Normality tests evaluate whether a dataset adheres to a normal distribution. A dataset exhibits normal distribution if the Skewness and Kurtosis analysis values fall within the range of +/-2 (Hatem *et al*., 2022). The skewness analysis conducted in this study revealed a minimum value of -0.58 and a maximum value of 0.419. Likewise, the Kurtosis analysis yielded a minimum value of -0.637 and a maximum value of 1.847, indicating conformity with normality.

Mahalanobis distance (D^2) was employed to identify potential outliers within the data set. This metric quantifies the deviation of an observation from the center (mean) of the distribution. In outlier detection, observations with D^2 values corresponding to a p-value less than 0.05 are typically considered outliers (Ghorbani, 2019). In this study, none of the calculated D^2 values yielded a p-value below the 0.05 threshold. This finding suggests that the data set likely contains no statistically significant outliers.

Considering the self-reported nature of the data collection, a potential concern lies in common method bias (CMB) (Podsakoff *et al*., 2003). Harman's single-factor test was employed as a statistical assessment to mitigate this potential bias. Exploratory factor analysis (EFA) was conducted, forcing all observed variables to load onto a single unrotated factor. The resulting single factor explained only 29.018% of the total variance, falling below the recommended threshold of 50% (Pandey & Charoensukmongkol, 2019). This finding suggests that CMB is unlikely to be a significant threat to the validity of the results.

Principal component analysis (PCA) with Varimax rotation, a type of orthogonal rotation, was employed to extract underlying factors from the 24 survey items. Varimax rotation promotes interpretable factors with minimal overlap between them (Forina *et al*., 2005). Eigenvalues were initially obtained for each component to assess their explanatory power. Following common practices, factor loadings with absolute values below 0.3 were suppressed to enhance interpretability. However, none of the factor loadings fell below this threshold, indicating that all items contributed meaningfully to the underlying factors. Consequently, all 24 items were retained for further analysis..

Further assessment of the data's suitability for factor analysis involved examining the commonalities extracted from the exploratory factor analysis (EFA). All five identified factors possessed eigenvalues exceeding Kaiser's criterion of 1 (Kaiser & Caffrey, 1965). These factors explained a substantial portion of the total variance, accounting for 63.926% (refer to Appendix 1).

3.3 Measurement Model Assessment

As hypothesized by theoretical underpinnings, the study conducted a convergent validity test to evaluate the convergence of items within constructs. Model fit was the primary focus of the initial analysis, which was conducted using established indices. The Adjusted Goodness-of-Fit Index (AGFI), Normed-Fit Index (NFI), Comparative Fit Index (CFI), and Goodness-of-Fit Index (GFI) all exceeded 0.9 (GFI = 0.957, NFI = 0.955, AGFI = 0.942, CFI = 0.993). Simultaneously, the Root Mean Square Error of Approximation (RMSEA) decreased below the prescribed threshold (RMSEA = 0.02). Collectively, these suggest that the model is well-fitting. Convergent validity was additionally assessed by applying composite reliability (CR) and average variance extracted (AVE). All CR values exceeded 0.7, and all AVE values exceeded 0.5. Furthermore, the CR consistently surpassed the AVE (see Table 2). These results demonstrate that the variables within each scale effectively converge in capturing the fundamental constructs. (Hoyle, 2023).

Table 2. Convergent validity

Variables	CR	AVE	No. of items in the scale
Risk Management and Governance (RMG)	0.816	0.527	4
Training and Awareness (TRA)	0.844	0.522	5
Incident Response and Controls (IRC)	0.88	0.599	5
Technology and Analytics (TEA)	0.845	0.521	5
Control Measures and Policies (CMP)	0.846	0.525	5

Source: Authors (2024)

The discriminant validity, which guarantees the uniqueness of the studied constructs, was confirmed through a comparison study. This approach entailed assessing the Average Variance Extracted (AVE) of each construct in comparison to the Maximum Shared Variance (MSV) and Average Shared Variance (ASV) obtained for all pairings of constructs (Fornell & Larcker, 1981). The findings, as shown in Table 3, consistently indicated that the average variance extracted (AVE) of each construct was higher than both the maximum shared variance (MSV) and average shared variance (ASV). This provides strong evidence for the distinctiveness of the measurement model.

Table 3. Discriminant Validity

Variables	CR	AVE	MSV	MaxR(H)	RMG	TRA	TEA	CMP
RMG	0.816	0.527	0.197	0.821	0.726			
TRA	0.880	0.599	0.246	0.895	0.444	0.774		
TEA	0.845	0.521	0.246	0.846	0.371	0.441	0.722	
CMP	0.846	0.525	0.236	0.855	0.390	0.486	0.374	0.725
IRC	0.844	0.522	0.246	0.860	0.393	0.896	0.496	0.483

Source: Authors (2024)

4. Results and Discussion

4.1 Model specification and regression analysis

This study employs an ordered probit regression model to examine the influence of various factors on Effective Fraud Prevention and Management (EFPM). This model is particularly suited for analysing the relationship between an ordinal dependent variable, like EFPM with ordered categories and multiple independent variables (Della Lucia *et al.*, 2013). The ordinal nature of EFPM implies a natural order among its categories; however, the intervals between them may not be equal.

The ordered probit model is formally specified as:

$Yi = \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + ... + \beta_iX_i + \epsilon_i$ (1)

Where:

- Yi represents the outcome variable with multiple categories (5 categories)
- X1, X2, X3, ..., Xi represents the independent variables.
- β_0 denotes the intercept term.
- β1, β2, ..., βi represent the coefficients for the corresponding independent variables.
- ϵi represents the error term.

The probability of Y being in each category given a specific value of X can be calculated using the cumulative distribution function (CDF) of the standard normal distribution (Φ).

For each category k (where k = 1 to 5):

$P(y = k \mid X) = \Phi(\mu_k - \beta_k * X$ (2)

This equation calculates the probability of Y being in category k given the values of the independent variables X and the corresponding coefficients β.

For the last category (k = 5):

$P(y = 5 \mid X) = 1 - \Sigma(\Phi(\mu_i - \beta_i * X))$ for i = 1 to 4 (3)

This equation calculates the probability of Y being in the last category (5) given X. It's computed by subtracting the sum of probabilities of all other categories from 1.

In these equations:

- μ_k represents the threshold for category k.
- β_k represents the coefficient of the independent variable X_k.
- $\Phi(\mu_k - \beta_k * X)$ represents the cumulative probability of Y being in category k, given the specific value of X.
- $\Sigma(\Phi(\mu_i - \beta_i * X))$ iterates over all categories from 1 to k-1 and calculates the cumulative probabilities for each category, excluding the last one.

STATA 13 was used for the statistical analyses. The independent variables in the model encompass Risk Management and Governance (RMG), Control Measures and Policies (CMP), Training and Awareness (TRA), Technology and Analytics (TEA) and Incident Response and Controls (IRC). The dependent variable is Effective Fraud Prevention and Management (EFPM).

This study analyses the impact of an independent variable (imputed using regression methods) on a five-level ordinal dependent variable representing effectiveness (Highly Ineffective to Highly Effective). We employ an ordered probit model to estimate the average change in the probability of achieving each effectiveness level for a one-unit increase in the independent variable, considering all observations in the sample.

4.2 Regression Analysis

Table 4 presents the ordered probit regression model, which includes 475 observations. The Wald chi-squared statistic is 102.46 with 5 degrees of freedom, and the associated p-value is less than 0.001. This indicates that the model is statistically significant overall, demonstrating that the independent variables collectively influence the dependent variable, Effective Fraud Prevention and Management (EFPM). Additionally, the Pseudo R-squared value of 0.398 suggests that the independent variables in the model explain approximately 39.8% of the variability in EFPM. Due to the nonlinearity of the equation in an ordered probit model, only the signs of the coefficients can be directly interpreted, not their magnitudes. To evaluate the quantitative effects of the independent variables, marginal effects are calculated. The results indicate a positive relationship between the constructs (CMP, RMG, IRC, TEA, TRA) and Effective Fraud Prevention Measures (EFPM)

Table 4. Ordered Probit regression

Variables	Coef.	Robust Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	1.242	0.235	5.3	0.00	0.783	1.702
RMG	1.148	0.264	4.34	0.000	0.630	1.665
IRC	1.155	0.236	4.89	0.000	0.692	1.619

TEA	1.145	0.180	6.36	0.00	0.792	1.489
TRA	0.928	0.186	4.95	0.00	0.561	1.296
Number of obs	475			Pseudo R2		0.398
Wald chi2(5)	142.46			Log pseudolikelihood		-357.52
Prob > chi2	<0.001					

Source: Primary data analysis output from STATA (2024)

4.3 *Ordered Probit Regression Marginal Effects*

Whether the marginal effects indicate a negative or positive sign, it is essential to understand that these signs reflect changes in the probability of EFPM falling into a specific category, given changes in the independent variables. However, the overall positive or negative relationship between the independent variables and EFPM should be determined by the sign of the regression coefficients from the ordered probit model. The marginal effects are conditional on the distribution across the categories of EFPM, meaning they represent the changes in the probability of being in a particular category rather than providing an absolute measure of the impact on fraud prevention effectiveness.

Table 5 revealed robust positive associations between all independent variables and the probability of achieving the highest effective fraud prevention measures (EFPM=5).

A one-unit increase in Control Measures and Policies (CMP) yields a statistically significant ($p < 0.001$) enhancement of approximately 27.62% in the probability of attaining the highest Effective Fraud Prevention Measures (EFPM) category, underscoring the substantial positive impact of comprehensive control measures and policies on optimal fraud prevention. Similarly, augmenting Risk Management and Governance (RMG) practices by one unit results in a statistically significant ($p < 0.001$) increase of roughly 25.51% in the probability of reaching the highest EFPM category, highlighting the critical importance of robust risk management and governance frameworks in fostering superior fraud prevention measures. Enhancements in Incident Response and Controls (IRC) also demonstrate a statistically significant ($p < 0.001$) positive effect, with a one-unit increase correlating with a 25.68% rise in the likelihood of achieving the highest EFPM category, emphasizing the crucial role of effective incident response and control practices. Additionally, a one-unit increase in Technology and Analytics (TEA) is associated with a statistically significant ($p < 0.001$) increase of approximately 25.46% in the probability of the highest EFPM category, underscoring the significant contribution of leveraging technology and analytics for optimal fraud detection. Finally, enhancing Training and Awareness (TRA) programs by one unit leads to a statistically significant ($p < 0.001$) increase of about 20.64% in the likelihood of attaining the highest EFPM category, highlighting the pivotal role of employee training and awareness in cultivating a culture of fraud prevention within organizations. These findings collectively emphasize the significant positive impact of strengthening various enterprise fraud risk management practices on achieving the highest effective fraud prevention measures.

Table 5. Marginal effects after ologit y = Pr(EFPM==5), predict(outcome(5))

Variables	dy/dx	Delta-method Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	0.276	0.049	5.59	0.00	0.179	0.373
RMG	0.255	0.054	4.68	0.000	0.148	0.362
IRC	0.257	0.048	5.32	0.000	0.162	0.351
TEA	0.255	0.037	6.90	0.00	0.182	0.327
TRA	0.206	0.041	5.09	0.00	0.127	0.286

Source: Primary data analysis output from STATA (2024)

Table 6 shows counterintuitive yet informative results concerning the impact of enterprise fraud risk management practices on the probability distribution of Effective Fraud Prevention Measures (EFPM). While all independent variables exhibited statistically significant ($p < 0.002$) negative associations with the probability of being in category 4 (EFPM=4), this can be reinterpreted as a positive shift towards achieving higher effectiveness categories.

A one-unit increase in Control Measures and Policies (CMP) leads to a decrease of approximately 6.07% in the probability of EFPM being in category 4. This suggests that implementing more robust CMPs effectively pushes the organization towards achieving higher levels of EFPM (category 5). Similarly, a one-unit increase in Risk Management and Governance (RMG) practices is associated with a decrease of 5.61% in the probability of EFPM being in category 4. This finding indicates that stronger RMG frameworks catalyze transitioning towards even more effective fraud prevention measures (category 5).

Strengthening Incident Response and Controls (IRC) by one unit also yields a decrease of 5.65% in the probability of category 4 EFPM. This implies that effective IRC practices contribute to a positive shift towards achieving higher levels of fraud prevention effectiveness (Category 5). Likewise, a one-unit increase in Technology and Analytics (TEA) is linked to a decrease of 5.60% in the probability of category 4 EFPM. This finding highlights that leveraging technology and analytics for fraud detection is instrumental in propelling organizations toward achieving more effective fraud prevention measures (categories 5 or above). Finally, a statistically significant decrease ($p < 0.002$) of 4.54% in the probability of category 4 EFPM is observed with a one-unit increase in Training and Awareness (TRA) programs. This suggests that enhanced employee training and awareness programs contribute to a positive shift towards achieving higher effectiveness in fraud prevention (categories 5 or above). Similar results for marginal effects with outcomes 3, 2, and 1 are presented in appendixes 2, 3, and 4.

Table 6. Marginal effects after ologit y = Pr (EFPM==4), predict (outcome (4)))

Variables	dy/dx	Delta-method Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	-0.061	0.018	-3.31	0.001	-0.097	-0.025
RMG	-0.056	0.017	-3.22	0.000	-0.090	-0.022
IRC	-0.056	0.016	-3.63	0.000	-0.087	-0.026
TEA	-0.056	0.015	-3.71	0.000	-0.086	-0.026
TRA	-0.045	0.015	-3.12	0.002	-0.074	-0.017

Source: Primary data analysis output from STATA (2024)

5. Conclusions

In conclusion, this analysis delved into the impact of various banks' fraud risk management practices on the probability of attaining a high level of effective fraud prevention measures (EFPM). As initially hypothesized, the findings unveiled a statistically significant positive correlation between all examined practices and achieving a superior EFPM category. The result indicates that bolstering practices such as Risk Management and Governance (RMG), Control Measures and Policies (CMP), Incident Response and Controls (IRC), Technology and Analytics (TEA), and Training and Awareness (TRA) contributes to organizations' effectiveness in combating fraud. These results underscore the significance of adopting a comprehensive approach to fraud risk management to establish a resilient defense against fraudulent activities within organizational settings. Compelling bank fraud prevention and management studies offer a win-win situation for all stakeholders. Banks benefit from reduced losses, improved reputation, and a more secure environment. Law enforcement gains valuable insights for combating fraud, and customers enjoy increased financial security and peace of mind.

While this research focuses on employee perceptions and utilizes a quantitative approach, a more generalized approach to bank fraud prevention should also consider the customer perspective. Future research could explore qualitative methods, such as interpretivism ontology and constructivist epistemology, to gain deeper insights into customer experiences and perceptions of fraud.

References

Abubakar, A. H. (2024). Evaluating the Impact of Training and Skill Development Programs on Employee Performance in Banking Sector / Financial Institutions. *Global Journal of Human Resource Management*, *12*(1), 1–10. https://doi.org/10.37745/gjhrm.2013/vol12n1110

Achary, R., & Shelke, C. J. (2023). Fraud Detection in Banking Transactions Using Machine Learning. *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, 221–226. https://doi.org/10.1109/IITCEE57236.2023.10091067

Ashraf, M., Abourezka, M. A., & Maghraby, F. A. (2022). *A Comparative Analysis of Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques* (pp. 267–282). https://doi.org/10.1007/978-981-16-2275-5_16

Asker, H., & Tamtam, A. (2020). An Investigation of the Information Security Awareness and Practices among

Third Level Education Staff, Case Study in Nalut Libya. *European Scientific Journal ESJ*, *16*(15). https://doi.org/10.19044/esj.2020.v16n15p20

Babbie, E. R. (2016). *The Practice of Social Research* (illustrate). Cengage Learning.

Byrapu Reddy, S. R., Kanagala, P., Ravichandran, P., Pulimamidi, D. R., Sivarambabu, P. V., & Polireddi, N. S. A. (2024). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors*, *33*, 101138. https://doi.org/10.1016/j.measen.2024.101138

Chau, D. H., & Faloutsos, C. (2018). Fraud Detection Using Social Network Analysis: A Case Study. In *Encyclopedia of Social Network Analysis and Mining* (pp. 856–861). Springer New York. https://doi.org/10.1007/978-1-4939-7131-2_284

Della Lucia, S. M., Minim, V. P. R., Silva, C. H. O., Minim, L. A., & Cipriano, P. D. A. (2013). Ordered probit regression analysis of the effect of brand name on beer acceptance by consumers. *Food Science and Technology*, *33*(3), 586–591. https://doi.org/10.1590/S0101-20612013005000068

Djamba, Y. K., & Neuman, W. L. (2002). Social Research Methods: Qualitative and Quantitative Approaches. *Teaching Sociology*, *30*(3), 380. https://doi.org/10.2307/3211488

Drogalas, G., Pazarskis, M., Anagnostopoulou, E., & Papachristou, A. (2017). The effect of internal audit effectiveness, auditor responsibility and training in fraud detection. *Journal of Accounting and Management Information Systems*, *16*(4), 434–454. https://doi.org/10.24818/jamis.2017.04001

Flowerastia, R. D., Trisnawati, E., & Budiono, H. (2021). *Fraud Awareness, Internal Control, and Corporate Governance on Fraud Prevention and Detection*. https://doi.org/10.2991/assehr.k.210805.038

Forina, M., Armanino, C., Lanteri, S., & Leardi, R. (2005). Methods of varimax Rotation in factor analysis with applications in clinical and food chemistry. *Journal of Chemometrics*, *3*(S1), 115–125. https://doi.org/10.1002/cem.1180030504

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.1177/002224378101800313

Ghorbani, H. (2019). MAHALANOBIS DISTANCE AND ITS APPLICATION FOR DETECTING MULTIVARIATE OUTLIERS. *Facta Universitatis, Series: Mathematics and Informatics*, 583. https://doi.org/10.22190/FUMI1903583G

Goodenough, A., & Waite, S. (2012). Real world research: a resource for users of social research methods in applied settings (3rd ed.). *Journal of Education for Teaching*, *38*(4), 513–515. https://doi.org/10.1080/02607476.2012.708121

Hatem, G., Zeidan, J., Goossens, M., & Moreira, C. (2022). NORMALITY TESTING METHODS AND THE IMPORTANCE OF SKEWNESS AND KURTOSIS IN STATISTICAL ANALYSIS. *BAU Journal - Science and Technology*, *3*(2). https://doi.org/10.54729/KTPE9512

Hoyle, R. H. (2023). *Handbook of Structural Equation Modeling* (R. H. Hoyle (ed.); Second). The Guilford Press.

HUSSAINI, U., BAKAR, A. A., & YUSUF, M.-B. O. (2018). The Effect of Fraud Risk Management, Risk Culture, on the Performance of Nigerian Banking Sector: Preliminary Analysis. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *8*(3). https://doi.org/10.6007/IJARAFMS/v8-i3/4798

Kaiser, H. F., & Caffrey, J. (1965). Alpha factor analysis. *Psychometrika*, *30*(1), 1–14. https://doi.org/10.1007/BF02289743

Knechel, W. R., & Willekens, M. (2006). The Role of Risk Management and Governance in Determining Audit Demand. *Journal of Business Finance & Accounting*, *33*(9–10), 1344–1367. https://doi.org/10.1111/j.1468-5957.2006.01238.x

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). *Cyber Security Awareness and Its Impact on Employee's Behavior* (pp. 103–111). https://doi.org/10.1007/978-3-319-49944-4_8

Magioli Sereno, M., & Ang, H. B. (Andy). (2024). The impact of gamification on training, work engagement, and job satisfaction in banking. *International Journal of Training and Development*. https://doi.org/10.1111/ijtd.12324

Musyoki, K. M. (2023). Internal Control Systems and their role in Financial Fraud Prevention in Kenya. *African Journal of Commercial Studies*, *3*(3), 173–180. https://doi.org/10.59413/ajocs/v3.i3.4

Ngigi Nyakarimi, S., Nduati Kariuki, S., & ’ombe Kariuki, P. W. (2020). Risk Assessment and Fraud Prevention in Banking Sector. *The Journal of Social Sciences Research*, *61*, 13–20. https://doi.org/10.32861/jssr.61.13.20

Olaniyan, R., Rakshit, S., & Vajjhala, N. R. (2023). *Application of User and Entity Behavioral Analytics (UEBA)* *in the Detection of Cyber Threats and Vulnerabilities Management* (pp. 419–426). https://doi.org/10.1007/978-981-19-8493-8_32

Olubusola Odeyemi, Noluthando Zamanjomane Mhlongo, Ekene Ezinwa Nwankwo, & Oluwatobi Timothy Soyombo. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, *11*(1), 2101–2110. https://doi.org/10.30574/ijsra.2024.11.1.0279

Omar, M., Nawawi, A., & Puteh Salin, A. S. A. (2016). The causes, impact and prevention of employee fraud. *Journal of Financial Crime*, *23*(4), 1012–1027. https://doi.org/10.1108/JFC-04-2015-0020

Pandey, A., & Charoensukmongkol, P. (2019). Contribution of cultural intelligence to adaptive selling and customer-oriented selling of salespeople at international trade shows: does cultural similarity matter? *Journal of Asia Business Studies*, *13*(1), 79–96. https://doi.org/10.1108/JABS-08-2017-0138

Philip Olaseni Shoetan, Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, & Onyeka Chrisanctus Ofodile. (2024). REVIEWING THE ROLE OF BIG DATA ANALYTICS IN FINANCIAL FRAUD DETECTION. *Finance & Accounting Research Journal*, *6*(3), 384–394. https://doi.org/10.51594/farj.v6i3.899

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. *Procedia - Social and Behavioral Sciences*, *145*, 97–102. https://doi.org/10.1016/j.sbspro.2014.06.015

Ramadhan, D. (2020). ROOT CAUSE ANALYSIS USING FRAUD PENTAGON THEORY APPROACH (A CONCEPTUAL FRAMEWORK). *Asia Pacific Fraud Journal*, *5*(1), 118. https://doi.org/10.21532/apfjournal.v5i1.142

Rashid, C. A. (2022). The role of internal control in fraud prevention and detection. *Journal of Global Economics and Business*, *3*(8), 43--55. https://doi.org/10.31039/jgeb.v3i8.40

Rehman, A., & Hashim, F. (2020). Impact of Fraud Preventive Measures on Good Corporate Governance. *Journal of Corporate Governance Research*, *4*(1), 35. https://doi.org/10.5296/jcgr.v4i1.17490

Rohmatin, B. L., Apriyanto, G., & Zuhroh, D. (2021). The Role of Good Corporate Governance to Fraud Prevention: An analysis based on the Fraud Pentagon. *Jurnal Keuangan Dan Perbankan*, *25*(2). https://doi.org/10.26905/jkdp.v25i2.5554

Samuel Onimisi Dawodu, Adedolapo Omotosho, Odunayo Josephine Akindote, Abimbola Oluwatoyin Adegbite, & Sarah Kuzankah Ewuga. (2023). CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES. *Computer Science & IT Research Journal*, *4*(3), 220–243. https://doi.org/10.51594/csitrj.v4i3.659

Shrestha, N. (2021). Factor Analysis as a Tool for Survey Analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), 4–11. https://doi.org/10.12691/ajams-9-1-2

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, *48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E. K., Alzboun, N., Al-Hawary, S. I. S., & Alshurideh, M. T. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science*, *8*(1), 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Williams et. al., A. (2019). Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. *International Journal of Computing and Digital Systems*, *8*(4), 387–396. https://doi.org/10.12785/ijcds/080407

Appendix 1: Total Variance Explained

Components	Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
TRA	7.652	31.884	31.884	3.337	13.906	13.906
TEA	2.240	9.332	41.216	3.182	13.257	27.163
CMP	1.960	8.167	49.383	3.106	12.943	10.106
IRC	1.799	7.497	56.879	3.089	12.869	52.975

RMG	1.691	7.047	63.926	2.628	10.951	63.926

Extraction Method: Principal Component Analysis.

Source: Primary data analysis output from SPSS (2024)

Appendix 2: Marginal effects after ologit y = Pr(EFPM==3), predict(outcome(3))

Variables	dy/dx	Delta-method Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	-0.166	0.030	-5.58	0.000	-0.224	-0.107
RMG	-0.153	0.033	-4.58	0.000	-0.218	-0.088
IRC	-0.154	0.032	-4.88	0.000	-0.216	-0.092
TEA	-0.153	0.022	-6.86	0.000	-0.193	-0.109
TRA	-0.124	0.023	-5.30	0.000	-0.170	-0.078

Source: Primary data analysis output from STATA (2024)

Appendix 3: Marginal effects after ologit y = Pr(EFPM==2), predict(outcome(2))

Variables	dy/dx	Delta-method Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	-0.039	0.009	-4.18	0.000	-0.057	-0.0205
RMG	-0.037	0.010	-3.64	0.000	-0.055	-0.0164
IRC	-0.036	0.009	-3.98	0.000	-0.054	-0.0182
TEA	-0.036	0.009	-4.09	0.000	-0.053	-0.1845
TRA	-0.028	0.008	-3.75	0.000	-0.044	-0.014

Source: Primary data analysis output from STATA (2024)

Appendix A4: Marginal effects after ologit y = Pr(EFPM==1), predict(outcome(1))

Variables	dy/dx	Delta-method Std. Err.	z	P>|z|	[95% Conf. Interval]	
CMP	-0.011	0.004	--2.56	0.000	-0.020	-0.0026
RMG	-0.010	0.004	-2.41	0.016	-0.019	-0.0019
IRC	-0.010	0.004	-2.56	0.011	-0.018	-0.0024
TEA	-0.010	0.004	-2.73	0.006	-0.018	-0.0029
TRA	-0.008	0.003	-2.56	0.010	-0.015	-0.0020

Source: Primary data analysis output from STATA (2024)