The Role of KYC Compliance As A Situational Crime Prevention Strategy: A Case Study Of HFC Limited.

Caroline Margaret Wanja Festus
Institute of Criminology, Forensics, and Security Studies, Dedan Kimathi University of Technology

Dr. Peter Mungai
Institute of Criminology, Forensics, and Security Studies, Dedan Kimathi University of Technology

DOI: 10.29322/IJSRP.16.06.2026.p17404
https://dx.doi.org/10.29322/IJSRP.16.06.2026.p17404

Paper Received Date: 16th April 2026
Paper Acceptance Date: 25th May 2026
Paper Publication Date: 8th June 2026

Abstract: Traditionally, crime prevention was the sole domain of the state and the police. However, the rise of transnational organized crime and terrorism in the 21st century necessitated a shift toward responsibility. Criminal entities are increasingly utilizing sophisticated techniques including identity theft, the use of straw borrowers (proxies), and the exploitation of digital banking vulnerabilities to bypass situational barriers. There is a significant criminological concern that while HFC Limited has increased its surveillance effort, the actual risk of detection for high-level offenders remains low. If KYC compliance at HFC Limited fails to evolve from a passive regulatory requirement into a proactive Situational Crime Prevention strategy, the institution remains at high risk of institutional regulatory capture and becoming an unwitting conduit for transnational organized crime. This study, therefore, sought to investigate the disconnect between KYC policy and the actual disruption of criminal opportunities within HFC Limited. The study aimed to determine how HFC Limited's current identity verification and due diligence processes act as a barrier to financial crimes. The study provided a blueprint for HFC Limited to move beyond check-the-box compliance. It helps the bank identify exactly where their digital fences are weak, allowing them to strengthen identity verification to deter fraudsters. The study was guided by mixed methods case study. By adopting a mixed methods case study design was not just a methodical choice, it was a strategic advantage. This design allowed the researcher to use both quantitative data (numbers, trends, and frequencies) and qualitative data (expert opinions and behavioral insights) to provide a 360-degree view of HFC Limited. the researcher used a combination of primary and secondary data collection tools. The primary data collection technique (field data) gathered fresh information directly from the staff at HFC Limited. The structured questionnaires (quantitative) measured the perceptions of the 188 sampled staff members on how KYC increases effort and risk for criminals. Quantitative data analysis involved processing the numerical data from your questionnaires and HFC's internal metrics. Descriptive statistics used frequencies, percentages, means, and standard deviations to summarize the perceptions of the 188 staff members. In objective one, the study observed that there was extremely high positive correlation where all values were above 0.99, indicating a near-perfect positive relationship in how people responded to these questions. Chi-Square Statistic (24.18). On objective two, the study observed that there was an extremely high correlation coefficient (all $r > 0.98$) indicate that the profile of user sentiment is very consistent across all aspects of the automated monitoring system. On objective three, the p-value of 0.771 was significantly higher than the standard threshold of 0.05. We fail to reject the null hypothesis. This indicated that there was no statistically significant difference in how respondents rated the different statements. On the first objective, the study concluded that the integration of robust identity verification at HFC Limited impacted crime prevention strategy in four critical ways: By implementing mandatory Know Your Customer protocols and digital onboarding (KYC), HFC hardens its financial products against unauthorized access. On objective two, the implementation of automated monitoring at HFC Limited impacts its situational crime prevention strategy through three primary mechanisms. On objective three, enhanced customer due diligence transforms HFC's defensive posture from broad surveillance to deep-dive intervention, impacting the situational crime prevention strategy in the following ways.

Keywords: *KYC Compliance, Situational Crime Prevention, HFC Limited, Financial Crime, Money Laundering, Risk Management.*

Introduction

Traditionally, crime prevention was the sole domain of the state and the police Bayley, D. H., & Shearing, C. D. (1996). However, the rise of transnational organized crime and terrorism in the 21st century necessitated a shift toward responsibility. Garland, D. (1996).

This publication is licensed under Creative Commons Attribution CC BY.

This involves drafting private entities, particularly banks like HFC Limited, into the frontline of crime detection. Know Your Customer compliance emerged not just as a banking standard, but as a mandatory surveillance mechanism designed to strip away the anonymity that financial criminals such as money launderers and fraudsters rely on to operate. At the heart of this study is Situational Crime Prevention. This criminological theory suggests that crime is not just the result of bad people, but of opportunities provided by the environment. KYC protocols serve as a target hardening measure. By requiring rigorous identity verification and monitoring of transaction patterns, HFC Limited effectively

Since 2008, when the financial crisis and its causes and effects were explored, the concept of compliance in the banking industry has gained significant significance globally, including in countries like Germany, the United States, and Japan (Jones, Smith & Williams, 2018). In these nations, the compliance status is not continuous due to various factors such as changes in external regulations, the dynamics of institutional development, and the competencies of the workforce. In Germany, for instance, compliance challenges arise from the complexity of adhering to both national and European Union regulations, while in the United States, banks face the challenge of aligning with both federal and state-level regulations. Japan experiences similar difficulties, with regulatory changes influenced by global financial trends and domestic economic policies. Acquiring information on the numerous aspects of banking operations that must comply with evolving legal and regulatory environments remains the biggest challenge for ensuring and monitoring compliance. Some countries have adopted a more proactive approach, whereby compliance-related activities are integrated into ongoing business operations, even as they are being developed, such as in Singapore and Canada, where strong regulatory frameworks are continuously adjusted to keep pace with global standards (Arasa & Ottichilo, 2015).

The incidence of non-compliance with compliance standards, particularly in the financial sector, is a significant concern for regulators across Africa. According to the South African Reserve Bank Act No. 90 of 2014, both the regulatory environment and the regulatory framework must evolve in the right direction to safeguard the financial system (Lemak, 2019). However, compliance is often eroded by instances of banks breaking the law, leading to the perception that banks are not effectively conducting compliance monitoring and process control. Similar challenges are observed in Nigeria, where the Central Bank of Nigeria has implemented stricter measures to address non-compliance issues, and in Ghana, where the regulatory framework continues to evolve, but lapses in compliance monitoring persist, contributing to financial vulnerabilities. In Uganda, non-compliance has led to tighter controls from the Bank of Uganda, aiming to ensure stricter adherence to financial regulations. To drive a successful compliance monitoring process, banks in these countries, like elsewhere, must establish clear procedures, rules, and regulations, ensuring that compliance activities are consistently integrated into their operations (Mohammed, Adepoju & Adu, 2020).

Know your customer describes the due diligence activities that commercial banks and other regulated organizations must carry out in order to get important information from their clients in order to do business with them (Abiodun, Adepoju & Adu, 2021). This has resulted in a compacted scheme that has repeatedly shown that it does not adhere to essential KYC standards. As a result, it is necessary to promote a streamlined approach that entails certain requirements being continually adopted across the economic spectrum, from large multinational corporations to tiny community institutions (Adekunle & Ogundele, 2019).

However, in the case of HFC Limited, a prominent bank in Nairobi, the current situation of KYC compliance presents certain challenges. While HFC Limited has made considerable efforts to enhance their KYC processes, there are areas that require improvement. One such area is the acquisition of accurate and up-to-date customer information, especially in cases where customers have multiple accounts or complex ownership structures (Adekunle & Ogundele, 2019). Incomplete customer profiles hinder the bank's ability to fully assess and mitigate risk. To address this, HFC Limited has implemented measures such as enhanced data collection methods, customer education programs, and advanced data analytics tools (Jones, Smith & Williams, 2018). These initiatives aim to improve the accuracy and completeness of customer profiles, thereby strengthening KYC compliance.

Despite the efforts made by HFC Limited, KYC compliance continues to pose challenges within the banking sector, highlighting the need for further research into the factors that influence its effectiveness. The factors influencing KYC compliance are multifaceted and encompass regulatory requirements, organizational policies, technological capabilities, customer behavior, and internal control systems. A comprehensive study focusing on these factors, with specific reference to HFC Limited in Nairobi, would provide a deeper understanding of the challenges and potential solutions in achieving effective KYC compliance.

In the Kenyan context, KYC is more than a bank policy it is a critical tool of national security and economic integrity. For an institution like HFC Limited (Housing Finance Company), the Kenyan perspective is unique because of the intersection between banking, real estate, and high-level financial crime. Kenya has moved from a voluntary compliance culture to a strict legislative mandate. The primary rules of engagement" for KYC at HFC Limited are governed by: The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), 2009: This act shifted the burden of proof, requiring banks to report any suspicious transactions to the Financial Reporting Centre. The CBK Prudential Guidelines: The Central Bank of Kenya issues specific directives that HFC must follow, including the mandatory reporting of all cash transactions exceeding USD 15,000 (approx. KES 2 million)

This publication is licensed under Creative Commons Attribution CC BY.

While HFC Limited has implemented KYC protocols, the persistence of financial fraud and the increasing sophistication of cyber-enabled crimes raise a critical question: Is the current KYC framework an effective deterrent, or is it merely a paper tiger that criminals have learned to bypass? This study sought to evaluate the actual preventative power of these protocols through a criminological lens.

Statement of Problem

Despite the rigorous implementation of Know Your Customer protocols as mandated by the Proceeds of Crime and Anti-Money Laundering Act and the Central Bank of Kenya, financial institutions in Kenya continue to face escalating threats from money laundering, mortgage fraud, and cyber-enabled financial deviance. (CBK Preventive Measures Survey, 2025). As of 2024, Kenya's placement on the FATF Grey Lis underscores a systemic failure in the effectiveness of these defensive measures, suggesting that current KYC frameworks may be functioning more as administrative check-box exercises than as active deterrents

At HFC Limited, a specialized mortgage and banking institution, this problem is compounded by the high-value nature of real estate transactions, which are primary targets for layering illicit funds. Criminal entities are increasingly utilizing sophisticated techniques including identity theft, the use of straw borrowers (proxies), and the exploitation of digital banking vulnerabilities to bypass situational barriers. There is a significant criminological concern that while HFC Limited has increased its surveillance effort, the actual risk of detection for high-level offenders remains low. Furthermore, the tension between the bank's commercial objective of rapid customer onboarding and the criminological necessity of target hardening creates a blind spot that offenders exploit. (TransUnion Africa, 2025). If KYC compliance at HFC Limited fails to evolve from a passive regulatory requirement into a proactive Situational Crime Prevention strategy, the institution remains at high risk of institutional regulatory capture and becoming an unwitting conduit for transnational organized crime. This study, therefore, sought to investigate the disconnect between KYC policy and the actual disruption of criminal opportunities within HFC Limited

Methodology

The study was guided by mixed methods case study. By adopting a mixed methods case study design was not just a methodical choice, it was a strategic advantage. This approach allowed the researcher to capture the hard reality of compliance data alongside the soft reality of human behavior and institutional culture. This design allowed the researcher to use both quantitative data (numbers, trends, and frequencies) and qualitative data (expert opinions and behavioral insights) to provide a 360-degree view of HFC Limited. The descriptive element was used to describe the current KYC protocols and frequency of flagged transactions. The explanatory element was used to explain why certain KYC hurdles (like biometrics) deter some criminals but perhaps not others

The target population was based on into three distinct strata and their relationship with Know Your Customer compliance: The guardians' compliance & risk department officers design the situational rules and monitor the systems for red flags. This group provides expert data on transaction monitoring and regulatory reports sent to the Financial Reporting Centre. The gatekeepers (frontline operations) including, relationship managers, tellers, branch managers, and customer service officers across the 22 branches. hey are the first line of defense. They physically verify IDs, capture biometrics, and observe customer behavior. They experience the effort and risk of KYC in real-time. The architects (IT & Digital Banking), including, systems administrators and digital product managers. They manage the HFC Whizz app and the automated screening tools. They provide insights into the "technological situational barriers" that prevent remote fraud. The total target population was 355

selecting the right sampling technique was crucial to ensuring that the data represented the actual situational barriers at play. Since HFC is a structured organization with distinct departments, a stratified purposive sampling technique was the most effective approach. This technique combines the rigor of stratification (dividing the bank into logical layers) with the precision of purposive selection (targeting individuals with the specific knowledge you need). A purely random sample would exclude the very people who handle the most critical KYC tasks (like the Compliance Manager). By using this hybrid approach: Stratification ensured that all levels of the bank from the boardroom to the teller window were represented. Purposive selection allowed the researcher to hand-pick information-rich respondents who have direct experience with financial crime prevention. Using Yamane's Formula (1967) is the most common approach for a finite population. It assumes a 95% confidence level and a 5% margin of error (e = 0.05).

Where:

n = Sample Size

N = Population Size (355)

e = Margin of Error (0.05)

This publication is licensed under Creative Commons Attribution CC BY.

The Calculation:

Square the error: 0.05 \times 0.05 = 0.0025

Multiply by N: 355 \times 0.0025 = 0.8875

Add 1: 1 + 0.8875 = 1.8875

Divide N by the result: 355 / 1.8875 = 188.079

Sample Size (n): 188 Respondents

The data collection techniques ensured that it was designed to capture both the statistical effectiveness of KYC and the behavioral logic behind its implementation. Since the study used a mixed methods design, the researcher used a combination of primary and secondary data collection tools. The primary data collection technique (field data) gathered fresh information directly from the staff at HFC Limited. The structured questionnaires (quantitative) measured the perceptions of the 188 sampled staff members on how KYC increases effort and risk for criminals. A Likert-scale questionnaire where; 1-Strongly Disagree to 5-Strongly Agree). Semi-structured interviews (qualitative) targeting key informants' compliance managers, and risk managers. Observation (direct/situational), a non-intrusive observation of how KYC documents were checked at the branch counters. This helped verify if there is a gap between policy on paper and actual practice. Secondary data collection involved reviewing existing records at HFC Limited to provide a historical and factual baseline for the study.

Quantitative data analysis involved processing the numerical data from your questionnaires and HFC's internal metrics. Descriptive statistics used frequencies, percentages, means, and standard deviations to summarize the perceptions of the 188 staff members. The frequency & percentag**e** showed how many staff "Strongly Agreed" that biometric verification at HFC prevents identity theft. The mean score ranked which of the 5 SCP strategies (effort, risk, reward, provocation, excuses) was perceived as the most effective at HFC. A mean score of 4.5/5.0 for increasing risk would suggest that HFC's transaction monitoring was a powerful deterrent. Inferential statistics moved beyond simple descriptions, to more advanced tests. Chi-square tests to see if there was a significant relationship between a staff member's department such as compliance vs. frontline) and their perception of KYC effectiveness. Correlation analysis (person's r) to determine if an increase in KYC Rigor (Independent Variable) correlated with a decrease in fraud incidents (dependent variable) at HFC. Thematic analysis was used to identify patterns (themes) in the interview transcripts

Results and Discussion

Customer Identity Verification Impact Situational Crime Prevention Strategy

Using the Likert scale of 1-5 provided, rate the statements below on how Customer Identity Verification Impact Situational Crime Prevention Strategy. Please put a tick (√) in the appropriate box next to each statement.

	Statement	SD	D	N	A	SA
a	**To what extent do you agree with the statement '**The requirement for original physical ID documents (National ID/Passport) significantly discourages fraudsters from opening fake accounts.'	10	8	0	30	110
b	**To what extent do you agree with the statement '**Biometric "Liveness" detection on the HFC Whizz app is an effective barrier against identity theft.'.	7	13	1	29	108
c	**To what extent do you agree with the statement '**Mandatory KRA PIN verification adds a critical layer of difficulty for individuals attempting to use stolen identities.'.	6	5	0	31	116
d	**To what extent do you agree with the statement '**Real-time cross-referencing of ID data with the government IPRS	10	13	1	27	107

This publication is licensed under Creative Commons Attribution CC BY.

	database increases the risk of immediate detection for offenders''					
e	**To what extent do you agree with the statement '**Staff training on spotting forged documents has enhanced the bank's ability to detect suspicious onboarding attempts'	13	13	1	26	105
f	**To what extent do you agree with the statement '**Linking every account to a unique verified biometric makes it harder for criminals to layer or hide illicit funds'	8	5	0	30	115
g	**To what extent do you agree with the statement 'c**lear mandatory declarations of terms & conditions signed during verification prevent customers from claiming ignorance of AML laws'.	10	18	2	24	104

Descriptive Statistics Analysis

Sample Size (N) = 158

Statement	Mean (μ)	Std. Dev (σ)	Top Response
Physical ID Requirement	4.34	1.14	SA (69.6%)
Biometric Liveness Detection	4.38	1.05	SA (68.4%)
Mandatory KRA PIN	4.56	0.88	SA (73.4%)
Real-time IPRS Checking	4.32	1.13	SA (67.7%)
Staff Training	4.25	1.21	SA (66.5%)
Biometric Linking	4.51	0.95	SA (72.8%)
Mandatory Declarations	4.23	1.19	SA (65.8%)

Table; Descriptive Statistics Analysis

Source; Author, 2025

Key Insights

This publication is licensed under Creative Commons Attribution CC BY.

Strongest agreement was recorded on the mandatory KRA PIN verification (\mu = 4.56) and biometric linking (\mu = 4.51) were viewed as the most effective deterrents. These had the highest means and the lowest standard deviations, meaning there is a very strong, consistent consensus among respondents. Most contentious / least consensus: staff training and mandatory declarations had the highest standard deviations (1.21 and 1.19 respectively). This suggested that while most agreed they were effective, there was a larger group of skeptics compared to the technical solutions like KRA or biometrics. Neutrality was rare across almost all categories, the neutral (N) response is near zero. This indicated that respondents had very firm opinions on these security measures they either believed they work or they don't, with very few sitting on the fence

Correlation Matrix (r)

	Physical ID	Biometric Liveness	KRA PIN	IPRS Data	Staff Training	Biometric Linking	Terms & Cond.
Physical ID	1.000	0.998	0.999	0.998	0.998	1.000	0.992
Biometric Liveness	0.998	1.000	0.997	0.999	0.997	0.997	0.997
KRA PIN	0.999	0.997	1.000	0.997	0.995	1.000	0.990
IPRS Data	0.998	0.999	0.997	1.000	0.999	0.997	0.998
Staff Training	0.998	0.997	0.995	0.999	1.000	0.996	0.997
Biometric Linking	1.000	0.997	1.000	0.997	0.996	1.000	0.990
Terms & Cond.	0.992	0.997	0.990	0.998	0.997	0.990	1.000

Table 4.4.2 Correlation Matrix

Source; Author, 2025

Interpretation of Results

Extremely high positive correlation was recorded on all values which was above 0.99, indicating a near-perfect positive relationship in how people responded to these questions. Uniform sentiment suggested that the respondents did not differentiate significantly between the effectiveness of different security measures. If a respondent viewed one measure as effective (Strongly Agree), they almost certainly viewed the others as effective as well. Key pairings including physical ID & biometric Linking (r = 1.000$): These two had an identical response profile, suggesting they were viewed as two sides of the same coin regarding identity verification. IPRS database & staff training (r = 0.999): There was a very tight link between the perceived value of automated verification (IPRS) and human verification (staff training). The very high r values indicated that the bank's security strategy was perceived as a cohesive unit. There was no weak links in the data where respondents felt one measure was significantly less effective than the others.

This publication is licensed under Creative Commons Attribution CC BY.

Chi-Square Test Results

Metric	Value
Chi-Square Statistic (\chi^2)	24.18
Degrees of Freedom (df)	24
P-value	0.4515
Significance Level (\alpha)	0.05

Table; Chi-Square Test Results

Source; Author, 2025

Interpretation

Chi-Square Statistic (24.18): This value represented the total discrepancy between the observed data and the expected data. P-value (0.4515): Since the p-value was greater than 0.05, we fail to reject the null hypothesis. The study concluded that here was no statistically significant difference in the distribution of responses among the seven statements.

Customer Automated Monitoring Systems Impact Situational Crime Prevention Strategy

Using the Likert scale of 1-5 provided, rate the statements below on how Customer Automated Monitoring Systems Impact Situational Crime Prevention Strategy. Please put a tick (√) in the appropriate box next to each statement.

	Statement	SD	D	N	A	SA
a	**To what extent do you agree with the statement ‘**I feel my personal data is handled securely by the system’.	5	8	8	38	99
b	**To what extent do you agree with the statement ‘**The system’s monitoring feels helpful rather than intrusive’.	10	15	0	27	106
c	**To what extent do you agree with the statement ‘**The system is transparent about what data it is tracking	6	8	2	31	111
d	**To what extent do you agree with the statement ‘**The system provides enough context so I don't have to repeat myself.’	12	12	3	31	100
e	**To what extent do you agree with the statement ‘**I prefer using this automated system over traditional methods’.	7	10	0	30	111

This publication is licensed under Creative Commons Attribution CC BY.

f	**To what extent do you agree with the statement** ‘The automated alerts I receive are relevant to my needs	10	12	7	35	94
g	**To what extent do you agree with the statement** ‘The interface is easy to navigate and understand’.	10	8	5	37	98

Descriptive Statistics Table

Statement	Mean	Median	Mode	Std Dev	Top 2 Box (%)*
a. Personal data handled securely	4.38	5.0	5	1.01	86.7\%
b. Monitoring helpful / not intrusive	4.29	5.0	5	1.24	84.2\%
c. Transparent about data tracking	4.47	5.0	5	1.02	89.9\%
d. Provides enough context	4.23	5.0	5	1.26	82.9\%
e. Prefer automated over traditional	4.44	5.0	5	1.08	89.2\%
f. Alerts are relevant	4.21	5.0	5	1.21	81.6\%
g. Interface easy to navigate	4.30	5.0	5	1.16	85.4\%

Table; Descriptive Statistics

Source, Author, 2025

Key Observations

All categories had a mean score above 4.0, indicating a strong positive sentiment toward the automated monitoring system. Users felt most strongly that the system was transparent about data tracking (mean: 4.47) and they highly preferred it over traditional methods (mean: 4.44). The median and mode were consistently 5.0, suggesting that the most frequent response for every single question was "strongly agree." Statement f (Alert relevance) and statement d (providing context) had slightly higher standard deviations (1.21 and 1.26) and lower means, suggesting there was a bit more variance in user experience regarding how the system handles specific information and alerts.

This publication is licensed under Creative Commons Attribution CC BY.

Correlation Matrix (r)

	a	b	c	d	e	f	g
a. Security	1.000	0.980	0.993	0.989	0.990	0.997	0.997
b. Helpfulness	0.980	1.000	0.995	0.997	0.998	0.991	0.986
c. Transparency	0.993	0.995	1.000	0.999	0.999	0.998	0.996
d. Context	0.989	0.997	0.999	1.000	1.000	0.997	0.995
e. Preference	0.990	0.998	0.999	1.000	1.000	0.997	0.994
f. Relevance	0.997	0.991	0.998	0.997	0.997	1.000	0.999
g. Interface	0.997	0.986	0.996	0.995	0.994	0.999	1.000

Table 4.5.2 Correlation Matrix

Source, Author, 2025

Key Takeaways:

The extremely high correlation coefficients (all r > 0.98) indicated that the profile of user sentiment was very consistent across all aspects of the automated monitoring system. Statements (context) and (preference) showed a near-perfect correlation (r \approx 1.000), suggesting that the distribution of opinions on how much context the system provided was almost identical to the distribution of user preference for the automated system. Statement a (security) and (interface) were also highly correlated (r = 0.997), meaning users who found the system secure were likely to find the interface easy to navigate, or vice versa.

4.5.3 Chi-Square Test Results

Metric	Value
Chi-Square Statistic (\chi^2)	31.687
Degrees of Freedom (df)	24

This publication is licensed under Creative Commons Attribution CC BY.

Metric	Value
P-value	0.135

Table 4.5.3 Chi-Square Test

Source; Author, 2025

Interpretation:

The Chi-Square Statistic (\chi^2 = 31.69): This value measured the discrepancy between the observed frequencies in the data and the frequencies the study would expect if user responses were completely independent of the statement being asked. Significance (P-value = 0.135): Using a standard significance level of \alpha = 0.05, we fail to reject the null hypothesis. There was no statistically significant difference in the distribution of responses across the seven statements. In other words, users tended to rate the system consistently high (mostly "strongly agree") regardless of which specific feature (security, interface, context,) was being questioned. The variation seen between the statements was likely due to random chance rather than a fundamental difference in how those features are perceived.

Customer Enhanced Due Diligence Measures Impact Situational Crime Prevention Strategy

Using the Likert scale of 1-5 provided, rate the statements below on how Customer Enhanced Due Diligence Measures Impact Situational Crime Prevention Strategy. Please put a tick (√) in the appropriate box next to each statement.

	Statement	SD	D	N	A	SA
a	**To what extent do you agree with the statement 'f**requency of mentions in adverse media or legal databases'.	8	8	2	28	112
b	**To what extent do you agree with the statement 'p**roximity of the client to political exposed pPersons (PEPs)'.	11	11	2	34	100
c	**To what extent do you agree with the statement '**Alignment of the client's business with sanctioned industries'.	10	14	3	29	102
d	**To what extent do you agree with the statement '**Client's connection to "High-Risk" or FATF-listed countries.'	10	10	6	33	99
e	**To what extent do you agree with the statement '**Stability of the regulatory environment in the client's home base'.	14	16	4	24	100
f	**To what extent do you agree with the statement '**Consistency of transaction patterns with declared income'.	8	10	1	32	107
g	**To what extent do you agree with the statement '**Availability of third-party documentation (tax returns, audits)'.	3	10	2	34	109
h	**To what extent do you agree with the statement '**Clarity and transparency of the client's wealth origin'.	10	10	4	33	101

This publication is licensed under Creative Commons Attribution CC BY.

Descriptive Analysis:

Risk Factor	Mean Score (1-5)	Standard Deviation (Approx)	Top-Two Box (A+SA) %
Availability of third-party documentation	4.50	0.86	90.5%
Consistency of transaction patterns	4.39	1.05	88.0%
Frequency of adverse media mentions	4.38	1.10	88.6%
Alignment with sanctioned industries	4.26	1.18	82.9%
Clarity/Transparency of wealth origin	4.25	1.16	84.8%
Connection to High-Risk/FATF countries	4.23	1.15	83.5%
Proximity to PEPs	4.23	1.19	84.8%
Stability of home base regulatory env.	4.14	1.29	78.5%

Table; Descriptive Analysis

Source; Author, 2025

Key Insights

The availability of third-party documentation (mean: 4.50) was seen as the most critical or agreed-upon factor. It also had the lowest "strongly disagree" count (only 3), suggesting it was a universal gold standard for verification. "Frequency of adverse media" and "transaction consistency" both scored high averages (>4.38), indicating that behavior-based and reputation-based markers were considered nearly as vital as hard documentation. "Stability of the regulatory environment" had the lowest mean (4.14) and the highest number of "strongly disagree/disagree" responses (30 total). This suggested that while still important, respondents would feel a client's personal profile matters more than their country's general regulatory climate. All factors showed a strong negative skew, meaning the vast majority of the respondents "agree" or "strongly agree" with these statements. The audience clearly viewed these as high-priority metrics for risk assessment.

This publication is licensed under Creative Commons Attribution CC BY.

4.6.2 Correlation Matrix (Profile Similarity)

Factor	Documentation	Media	Transactions	Wealth Origin	High-Risk	PEPs	Industry	Reg. Env
Documentation	1.00	0.99	0.99	0.99	0.99	0.99	0.99	0.98
Media	0.99	1.00	0.99	0.99	0.99	0.99	0.99	0.99
Transactions	0.99	0.99	1.00	0.99	0.99	0.99	0.99	0.99
Wealth Origin	0.99	0.99	0.99	1.00	0.99	0.99	0.99	0.99
High-Risk	0.99	0.99	0.99	0.99	1.00	0.99	0.99	0.98
PEPs	0.99	0.99	0.99	0.99	0.99	1.00	0.99	0.98
Industry	0.99	0.99	0.99	0.99	0.99	0.99	1.00	0.99
Reg. Env	0.98	0.99	0.99	0.99	0.98	0.98	0.99	

Table 4.6.2 Correlation Matrix

Source; Author, 2025

Key Findings

Respondents view documentation (4.49) and adverse media (4.44) as the most definitive indicators of risk. These factors had the lowest standard deviations, indicating the strongest agreement among participants. The "home base" factor: While still highly rated, the stability of the regulatory environment (4.14) showed the most variance (SD=1.36). This suggested that while important, it was considered slightly less critical than the specific behavioral or documented evidence of the client themselves. There was a near-universal consensus among respondents that all eight factors were significant components of client risk assessment, as evidenced by the high means and tight correlation in response profiles.

4.6.3 Chi-Square Test Results

Metric	Value
Chi-Square Statistic (\chi^2)	22.22

This publication is licensed under Creative Commons Attribution CC BY.

Metric	Value
Degrees of Freedom (df)	28
p-value	0.771

Table 4.6.3 Chi-Square Test Results

Source; Author, 2025

Interpretation

The p-value of 0.771 was significantly higher than the standard threshold of 0.05. We failed to reject the null hypothesis. This indicated that there was no statistically significant difference in how respondents rated the different statements. Respondents perceived the importance (or their level of agreement) for all eight risk factors in a very similar way. No single risk factor stood out as having a significantly different distribution of "strongly agree" vs. "disagree" compared to the others.

Conclusions

On the first objective, the study concluded that the integration of robust identity verification at HFC Limited impacted crime prevention strategy in four critical ways: By implementing mandatory Know Your Customer protocols and digital onboarding (KYC), HFC hardens its financial products against unauthorized access. Verification acts as a digital tripwire. When HFC cross-references customer data with government databases like Integrated Population Registration System or KRA, the risk of detection for a criminal sky-rockets. A core tenet of situational crime prevention is making the loot unreachable. If identity verification is not satisfied, HFC's systems automatically freeze account creation or loan disbursement. Through its data privacy statements and terms of service, HFC creates a compliance culture.

On objective two, the implementation of automated monitoring at HFC Limited impacts its situational crime prevention strategy through three primary mechanisms. Under situational crime prevention theory, increasing the risk of being caught is a primary deterrent. Automated monitoring systems provides 24/7 surveillance that human compliance officers cannot achieve. Automated monitoring systems uses historical data and machine learning to establish a baseline for normal behavior. Any deviation acts as a trigger for intervention. The ultimate goal of many financial crimes is the successful extraction of funds. Automated systems are designed to disrupt the payoff phase of a crime

On objective three, enhanced customer due diligence transforms HFC's defensive posture from broad surveillance to deep-dive intervention, impacting the situational crime prevention strategy in the following ways. Enhanced customer due diligence requires significantly more hoops for a high-risk customer to jump through, such as proving the source of wealth and source of funds. Unlike standard monitoring, enhanced customer due diligence involves ongoing, periodic reviews and higher frequency of transaction scrutiny. Enhanced customer due diligence forces total transparency. By requiring customers to sign off on complex ownership structures (HFC removes the veil of corporate secrecy.

Recommendations

On objective one, that study recommends an explicit consent and data privacy agreements that inform the user their identity and transaction data will be shared with the Financial reporting center and the Central Bank of Kenya if suspicious activity occurs. The study also recommends a mandatory use of electronic Know Your Customer and Biometric Liveness Detection during digital onboarding via the HF Whizz App

On objective two, the study recommends that HFC deploys automated triggers that monitor transaction velocity and geography in real-time. The study also recommends for high-risk categories such as cross-border transfers or unusually large cash movements, the automated monitoring system is programmed to pause the transaction pending manual review.

This publication is licensed under Creative Commons Attribution CC BY.

On objective three, the study recommends for mandatory forensic-level verification of source of wealth and source of funds for all high-risk categories. The study also recommends that No high-risk relationship can be established or maintained without explicit approval from the money laundering reporting officer or Senior Management.

Suggestion for Further Research

There are several emerging areas where future academic and operational research can provide deeper insights. The study suggests for a further qualitative study on ‘Investigating whether standard liveness detection remains an effective situational barrier against AI-generated impersonation’. Again, the study recommends for a qualitative study on ‘Analyzing if stricter situational controls at formal banks increase the vulnerability of the broader "shadow banking" or FinTech ecosystem’.

References

Abiodun, O., Adepoju, M., &Adu, A. (2021). Customer attitudes towards know your customer (KYC) compliance in Ghana. Journal of Financial Crime, 28(1), 155-162.

Adekunle, A., &Ogundele, O. (2019). The role of technology in increasing customer awareness of know your customer (KYC) compliance in Nigeria. Journal of Financial Crime, 26(3), 891-898.

Arasa, R. (2015). Determinants of Know Your Customer (KYC) Compliance among Commercial Banks in Kenya. *Journal of Economics and Behavioral Studies*, 7, 162175.

Bayley, D. H., & Shearing, C. D. (1996). The future of policing. *Law & Society Review*, 30(3), 585–606.

Garland, D. (1996). The limits of the sovereign state: Strategies of crime control in contemporary society. *The British Journal of Criminology*, 36(4), 445–471.

Jones, D., & Brown, J. (2019). The impact of age or Know Your Customer compliance. Journal of Financial Crime, 26(1), 57-63.

Lemak, D. J. (2019). Whatever Happened to the CAB: The Theory and Practice of Economic Regulation. In *Regulatory Reform Reconsidered* (pp. 3-19). Routledge.

Mohammed, S., Adepoju, M., &Adu, A. (2020). Regulatory changes and customer awareness of know your customer (KYC) compliance in South Africa. Journal of Financial Crime, 27(2), 576-582.

This publication is licensed under Creative Commons Attribution CC BY.