



Analysis of Internal Fraud in the Microloan Process with Confirmatory Factor Analysis (CFA) and the Extreme Gradient Boosting (XGBoost) Method

Heri Supriyadi¹(✉), Dominicus Savio Priyarsono², Dominicus Savio Priyarsono¹, and Trias Andati¹

¹ School of Business, IPB University, Bogor, Indonesia
lingga8122@yahoo.com

² Department of Economics, IPB University, Bogor, Indonesia

Abstract. Internal fraud in the microcredit business process has caused significant losses to the banking industry and financial institutions. Internal fraud is one type of operational risk frequently faced by banks/financial institutions focusing on microcredit services. The typical fraud frequently found is Corruption and Misappropriation of Assets (ACFE). For instance, ‘Tempilan’ credit, Mask credit, and Fictitious Credit. Machine learning automatically predicts the possibility of internal fraud in the microloan business process. This research aimed to determine which the most dominant component from the theory of social identity and the fraud triangle that influence someone to commit fraud is. The research used the CFA (Confirmatory Factor Analysis) method and the Extreme Gradient Boosting (XGBoost) method to predict the possibility of fraud. The results revealed that the fraud incident conducted by Relationship Managers (RM) is caused by rationalization factors. The Path diagram of the Second Order CFA fraud risk showed the marketer that the most significant factor loading value was in rationalization, followed by pressure and opportunity. Hence, the results of this research indicated that rationalization had the most significant influence on the fraud risk committed by RM. Therefore It was recommended that the bank or financial institution put its focus more on rationalization matters.

Keywords: CFA · Fraud · Mitigation · Prevention · Prediction · XGBoost

1 Introduction

The banking sector is dealing with a severe issue as the prevalence of fraud, integrity violations, and fraud is on the rise and growing more complex. Because of that, the authors recognizes how crucial it is to assess the banking sector’s readiness to implement efficient fraud-fighting measures. Fraud losses include both monetary costs for example the decline of firm profitability and non-financial losses such as harming bank reputation, decreasing bank soundness, and increasing risk profile levels. In addition, non-financial

losses include reputational/brand damage, loss of market position, negative investor sentiment, employee morale, and loss of future opportunities. Fraud is one of the most influential factors in the sustainability of the company's business. Furthermore, its trend from year to year tends to increase regardless of the size, profitability of the company, and its industry [1]. The company's business process automation, which is being intensively carried out in various industries, has opened up more fraud opportunities in the company. For this reason, fraud prevention and detection efforts are increasingly complex [2].

The data from the Association of Certified Fraud Examiners (ACFE) Indonesia mentioned that corruption was the highest fraud in 2019 and it was released for all institutions, including Government and corporate in 2020. Corruption was the top and it was followed by abuse of company/state assets. In addition, ACFE Indonesia revealed that losses due to fraud in 2019 reached IDR 873 billions with an average loss per case of IDR 7,2 billions. Of these losses, the financial and banking industries were the most disadvantaged, with a percentage reaching 41.40%, followed by the Government with 33.90%.

Fraud perpetrators can come from internal companies (internal fraud) or outside the company (external fraud). Fraud can also be distinguished based on the type of fraud related to misuse of data, embezzlement of assets, and manipulation of income and expenses, [3]. Fraud committed by employees (internal fraud) through business operational activities affected the sustainability of the future business through the deterioration of the company's reputation [4]. Fraud perpetrators can always take advantage of every opportunity, gap, or weakness in their controls, blatant dishonesty, and collusion [5]. Many efforts have been made to reduce the fraud, including strengthening internal control, implementing risk management, and improving audit quality. Considering what is being discussed above, it can be drawn the problem statement of the research in the following question: which is the most dominant component among opportunity, rationalization, and pressure (taken from the triangle fraud theory) in influencing the possibility of fraud in the microloan process in Indonesia? In summary, this research aims to answer the question by using the Confirmatory Factor Analysis (CFA) method.

2 Literature Review

There are several empirical and impactful studies on fraud in companies that have been done on efforts to reduce it. For example, the study on the motives behind fraud (red flags) and how fraud can be prevented and detected [1]. The results of the literature review by Mangala and Kumar summarize several researchers who have conducted studies related to fraud, which are grouped into theoretical dimensions: Fraud Triangle, Fraud Risk Assessment Hierarchy, Diamond Fraud, Pentagon Fraud, and 3C's Model. [6] in their research of fraud in financial institutions, stated that fraud is a fundamental problem, and even the Saudi Arabian banking sector is also not immune to this disease. The banking and insurance industries appear to be more exposed to money laundering risks [7].

Knowing the perpetrators and their motives for committing fraud is crucial to mitigate fraud risk. The Fraud Triangle is often used to describe the factors that make someone commit fraud [8]. Meanwhile, in the context of Indonesia banking, [9] has studied fraud to explore the motives of banking crimes [10] stated that although fraud is a global

issue for several cultures, the triggers are not universal. Therefore, [11] concluded that understanding the motives of fraud is the same as understanding the process of identifying the behavioral factors of fraud perpetrators. Companies must create an environment that upholds ethics and correct behavior in every activity. Fraud triangle analysis as a tool to evaluate fraud risk and its possibility is fundamental as it could reveal the fraudulent actions that have been carefully planned and their supportive behavior, including things that are difficult to do. Referring to the framework of the Fraud triangle and the theory of planned behavior, [10] presented a conceptual model of fraud behavior and explain that fraud can be triggered by different motives and influenced by the level of socio-cultural and cultural values of different individuals. In line with the concept of [10, 12] mentioned that corporate culture and the nature of the industry have a significant effect on the likelihood of fraud.

[13] found most of auditors used Internal control framework in assessing fraud risk tendencies. Besides, the auditors used the Fraud triangle elements to assess as it is the second basis for consideration after the internal control framework. [14] stated that financial pressure has a significant role in encouraging workers and bank managers to commit fraud. However, the form of financial pressure differs based on the type of work or job position in the bank. [9] mentioned that financial motives were the main reason perpetrators committed banking crimes.

Furthermore, [15] stated that financial pressure had a significant role in influencing bank employees and managers to commit fraud. The nature of this financial pressure differed significantly among the positions of the actors in the bank. However, [4] stated that there was no significant difference when viewed from the job position to commit fraud. In addition, fraud was mostly committed by men, new workers, and young employee. [16] concluded that adequate policies and SOPs can control internal fraud and wrong actions. However, these policies and SOPs will not be practical or even functional when the person in charge violates the policies and procedures themselves. They reiterated that the low level of compliance with internal control provides opportunities for fraud. Correspondingly, the management who ignores internal control has a higher risk of collusion in the company [17].

Weak internal banking supervision, inadequate internal control supervision, and customer trust in banking are viewed as opportunities by perpetrators. The assumption of the job position to act excessively (over-reaction) as well as the implementation of ineffective entity values are used as a justification for acting defiantly [9]. [18] concluded that the most effective fraud prevention and detection procedures are operational audits, internal control reviews, improvements, cash reviews, and code of sanctions against vendors and ethics officers. The most effective procedure for fraud prevention and detection is information technology.

According to [8], controlling chances to avoid fraud is crucial, and tightening internal controls in several ways can reduce fraud opportunities. Internal control only, however, would not be able to stop fraud since 20% of fraud acts are committed at random aside from the control issue and 11% of fraud acts are committed as there is a collusion to deceive internal control (fool control). Meanwhile, fraud committed by management cannot be dismissed because there is no control mechanism. The managements handling the internal control generally can act as their will such as ignoring control [19].

Furthermore, [20] concludes that borrowers must be aware that the risk of fraud will not stop when the loan has been booked or when the extension is made. Therefore, it is essential for banks to visit customers and they should be involved to control bank management.

On the other hand, [21] stated that the size of the audit firm, length of service, and level of experience of the auditor provide significant differences in predicting the possibility of fraud. The form of internal control over fraud that directly impacts marketing interests is researched by [22]. They present a positive relationship between customer knowledge regarding fraud prevention efforts and the quality of the company’s relationship with customers, as measured by customer satisfaction, trust, and commitment. They emphasized the importance of fraud prevention efforts in retail banks. Achieving financial goals such as lowering operational costs, fraud prevention, and effective communication is a significant way to improve the quality of customer loyalty.

Fraud is a critical issue in every financial institution, according to [6], who discussed the use of technology to improve fraud protection capacities. Technology advancements have prompted banks to build electronic banking service technology, posing new difficulties for combating bank fraud. His findings successfully created a framework for preventing fraud with administrative and technical restrictions. [23] have developed a concept known as the Ishikawa diagram. This chart can be used by company management or external auditors and internal auditors and risk officers in brainstorming to improve fraud prevention and detection capabilities. The diagram can explain, illustrate the causes of fraud that are not visible or hidden by sharing knowledge and ideas between team members and digging for more profound studies to obtain sufficient data.

Several previous studies have discussed a lot about red flags for Fraud occurrences in the company. Mangala and [1] have studied several kinds of Literature focusing on components that can be used as red flags (Fig. 1). In general, the components of red These flags can also be categorized in the following taxonomic form.

Source: Review of Literature by [1].

According to an empirical research on fraud, some signs may be observed before fraud happens [24]. These signs are red flags. Red flags are particular warning signs of prospective fraud situations. Red flags are situations that show the presence of chances

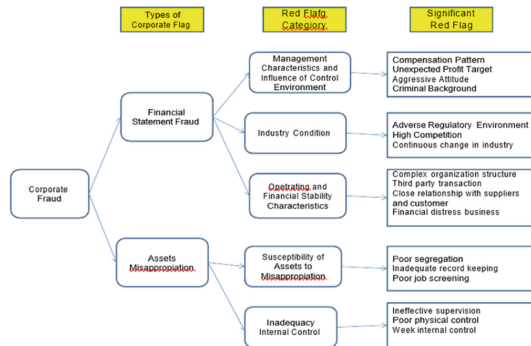


Fig. 1. Red Flags Taxonomy

and incentives for fraud. Red flags are a crucial tool for spotting fraud at an early stage. A particular worry for corporate owners is the rise of financial corporation scams. In order to create early warning systems for fraud, numerous financial institutions have started to consider the usage of red flags. Events or a group of circumstances that might notify an organization of fraud are known as red flags or signs of suspected fraud [5]. On the other hand, red flags are as an organized method to hone, reveal, and record fraud, suspected theft, and corruption so that they may be discovered more quickly and effectively. Early fraud detection might be detected from the signs of fraud, specifically for Indonesia circumstances. Weak internal control systems, discrepancies in accounting records, “strange” behavioral characteristics of fraud offenders, and frequent complaints cause these symptoms to manifest. There are a variety of other fraud red flags that can be employed.

The number of banks stumbling over fraud is still high every year. Based on the Triangle Fraud Cressey analysis, perpetrators’ primary motivation to commit banking crimes is financial reasons. An ineffective banking system and low internal and external supervision are considered an opportunity to commit crimes. The perpetrator justifies the meeting between motive and opportunity to justify his actions [9]. Although corruption will never be eradicated, it can be curbed and chances for it can be pressed. Governance and corruption at a garment bank, where a structure and system are built to help employees refrain from corruption and prevent it from an early stage. This research outlines various best practices in banks to reduce behavior that encourages corruption, including strict monitoring, decentralized authority, evaluation of decision-making processes, intense auditing, punitive measures, openness, and anti-corruption culture.

Meanwhile, [24] studied how microfinance organizations in Indonesia, like the BRI bank unit have communicated several facts concerning measures to reduce fraud. Internal control, internal audit, and financial processes have all been tightly enforced in the BRI Unit and by doing so the financial risk management of the bank is viable. Therefore, it can be inferred that internal control, auditing skills, and effective risk management are among the factors that affect BRI performance.

Data analytics is the science of extracting insights from big data collections to help people or organizations. Data analytics uses Machine Learning, Artificial Intelligence (AI), Statistics, and natural language processing techniques to find patterns in data. It utilizes data visualization tools and human-computer interaction to make these patterns understandable to users and refers to using analytics software to identify trends, patterns, anomalies, and exceptions in data. There are four types of Data Analytics. For instance, Descriptive Analytics or known as Business Intelligence, Diagnostic Analytics (to diagnose factors/causes of past performance), Predictive Analytics to predict future results, and Prescriptive Analytics as the most specific analytics to provide specific solutions. Big data, machine learning, AI, and cloud computing have pushed the financial industry towards digitization. Big data has revolutionized the financial industry, especially related to the accurate time in monitor the capital market, fraud detection and prevention, and accurate risk analysis through machine learning processes.

[35] included a series of methodologies that can manage various large-scale data-based problems faced by many entities, including government entities. It is an iterative process that connects several statistical methods, from data sampling, model estimation,

model prediction, and evaluation, to form an integrated system that can predict fraud, waste, violations, and some unexpected things [36]. Predictive Analytics aims to build analytical models that predict the target size of interest. These targets are used to direct the learning process during the optimization procedure. There are two types of predictive analytics depending on the size of the target, namely regression, and classification. An example of target variable in the regression is the amount of loss or limited to an interval.

Meanwhile, the target classification is categorical, the binary classification between fraud and non-fraud. In fraud detection, both types of regression and classification predictions can be used simultaneously. Some organizations have begun to increase their reliance on the algorithm-based decision-making to monitor their workers. This trend is supported by the technology industry providing confidence that their decision-making tools are efficient and objective. Furthermore, the predictive algorithm can present a score value that indicates the possibility of an event occurring. This tool can be used to identify suspicious worker behavior that has the potential to violate the company. An essential step in developing information for predictive analytics is setting the goal of the prediction itself. Meanwhile, other important things are Data Collection and Sampling, Model Estimation, Prediction and Model Evaluation, and Sampling and Model Adjustments.

Given that technology and organizations are constantly changing, the opportunities for fraud in companies will continually change. For this reason, reminds us that companies must routinely conduct assessments of the effectiveness of controls, prevention, and fraud detection tools. Fraud will continually develop as well as anti-fraud tools, including tools for predicting the occurrence of fraud, for that it is always necessary to maintain and improve effectiveness.

3 Method

This research has been implemented intensively from January 2020 to December 2022. It covered some activities such as research preparation (literature review), proposal preparation, data collection, data analysis process, and preparation of presenting research results in Jakarta. The authors adopted a hybrid quantitative and qualitative methodology. The degree of impact between the dependent variable and the independent variable was described and quantified in quantitative analysis. The number of controls was measured using the opportunity, rationalization, and pressure goal variables. The research also used operational factors. For example, the independent variable was broken down into opportunity, rationalization, and pressure variables. Meanwhile, the dependent variable is fraud. The method utilized to develop a plan for reducing the risk of fraud is the qualitative approach. This step used information on fraud in bank "X", a procedure that has been used, and compared the outcomes.

The data collection stage was started by conducting semi-structured interviews with the chosen stakeholders. The respondents were anticipated to know and be responsible for Bank 'X' microloan program. The authors gathered information, applied the fraud triangle theory to analyse, and run some tests in order to discover the conclusions that were related to one another. The authors's primary source of information was information on fraud incidences that occurred in 2017, 2018, and 2019. The fraud information included fictional loans, display loans, camouflaged loans, gratification, and late

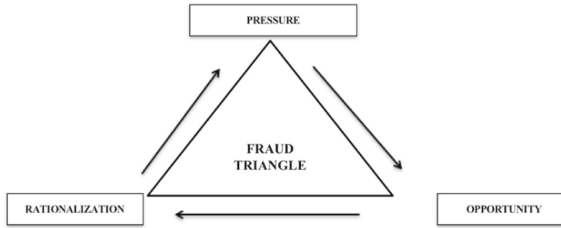


Fig. 2. Fraud Triangle Chart

installment payments from debtors. In addition, this research used profile data from all marketing officers or Relationship Managers (RM) obtained from the database at Bank X's head office in Jakarta. The data in question includes performance profile data—demographics, career paths, financial transactions, and financial liability data during the above research period.

Donald Cressey (1950) in his study concluded that three conditions cause a person to commit fraud. The three essential components of the Fraud Triangle are Opportunity, Rationalization, and Pressure, Fig. 2.

1. Pressure is a situation and condition that encourages individuals to commit fraud. Pressure covers many things, and one of the biggest is finance. Pressure can come from internal or external company parties – a condition where individuals are encouraged to commit fraud.
2. Rationalization or justification. Rationalization makes individuals who initially do not want to commit fraud tend to do so. Rationalization is personal as there is an element of justification for wrongdoing. Individuals who commit fraud tend to find justification for their actions.
3. Fraud can happen if the opportunity comes. The opportunity to commit fraud happens when it has a low risk of being known or detected by others.

Technology based on machine learning (ML) is frequently employed in attempts to stop fraud. The credit score model (also known as credit risk scoring or credit risk rating) is one of the instruments used to examine credit applications. The credit score model is often created using logistic regression (LR), which might be accepted or denied. In order to provide reliable modeling, machine learning models must also undergo training on historical data, particularly data linked to credit history and pertinent red flags. The ML model for significance evaluates each attribute before being converted into a prediction. Such an ML model's primary drawback is that it can only account for linear connections between the input and predicted variables. This model provides an interpretable framework for logistic regression. In credit risk modeling, this logistic regression model is often employed. By adding non-linearity to the model and identifying more complex dependant variables, ML enables the adoption of more advanced modeling approaches. Confirmatory Factor Analysis (CFA) used in this research to correctly identify the chosen variable before using the XGBoost model.

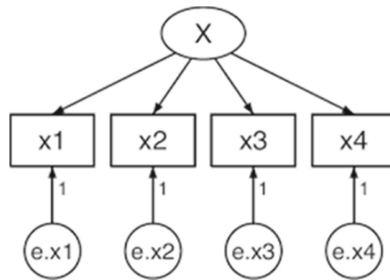


Fig. 3. Confirmatory Factor Analysis (CFA)

The confirmatory factor analysis is often called CFA. It is used to test the dimensionality of a construct or variable. In general, before analyzing the structural model, authors must first measure the model to test the validity and reliability of the indicators forming the construct or latent variable using CFA. A construct conceptually can be formed unidimensional and multi-dimensionally. If the construct is unidimensional, then testing the construct's validity can be done with First Order CFA. In contrast, Second Order CFA can be done if the variable is multidimensional. CFA is based on the observed variables being imperfect indicators of latent variables or certain underlying constructs. CFA is one of the two main approaches in factor analysis. In general, it can be considered that the CFA method is used to test the validity or confirm the theory in a model.

In many research cases, the first latent variable explains the second latent variable; if a model like this appears, the analysis used is Second Order CFA. This CFA model is also possible with higher levels or orders, for example, third-level confirmatory factor analysis, Fig. 3.

After obtaining the results whose data met the assumption of a multivariate normal distribution, the analysis was continued using the CFA method. The analysis was started from the second order risk of the RM committing fraud in order to get indicators that have a significant contribution. Then, it was proceeded with First Order CFA analysis on each latent variable to determine the validity-reliability and contribution given by each indicator variable in compiling the latent variable. In order to obtain a second-order model on the fraud risk of the marketers, Several experiments were carried out and all possible indicators were combined so that the optimum model results were obtained with indicators that met the goodness of fit criteria and were valid and reliable. The indicators were described in the following Table 1.

Table 1. Confirmatory Factor Analysis (CFA)

No	Statistics	Criteria
1	Minimum fit function chi-square (χ^2)	p_value > 5%
2	RMSEA (The Root Mean Square Error of Approximation)	< 0.08
3	RMR	< = 0.1
4	SRMR	< = 0.1
5	GFI (Goodness of FIT Index)	> = 0.9
6	AGFI	> = 0.9
7	NFI	> = 0.9
8	NNFI	> = 0.9
9	CFI (Comparative FIT Index)	> = 0.9
10	IFI	> = 0.9
11	RFI	> = 0.9
12	PNFI	> = 0.9

Table 2. Microcredit Loan Process

Procedure Stage	Potential Risk	Risk Mitigation
Analyzing and Proposing, inputting debtor data and documents and conducting 5C analysis through the application (system)	1. Document engineering 2. Analysis of the condition of the debtor is not fair	Applications for geo- tagging, document re- verification, business fairness, and ability to pay.
Approval and Disbursing: Re-verify the documents and data entered, and the authenticity of the collateral documents, and make credit decisions	1. The amount of credit is not suitable for other purposes 2. Loans used by others 3. Gratification by debtor	verification, Debtor's Repayment Capacity (RPC), fairness of the creditprocess, installation of SMS notifications to debtors, and tokens for OTP before deciding on credit.
Monitoring and Repayment: Officers regularly visit debtors to ensure business progress and further customer needs	Credit installments are not deposited/deferred by the officer.	Using online media

This research used the Construct Reliability (CR) method to conduct the reliability test. Reliability test was conducted to measure the internal consistency of the measuring instrument. The reliability shows a measuring instrument's accuracy, consistency, and

Table 3. Research variable

Triangle Components	Variable Name	Code	Data Type	Measurement Type	Var No
-	Status (Fraud/not)	Y	Qualitative	Dummy	1
Rationalization	Job Grade/ Position Level	X1	Qualitative	Attribute	2
Rationalization	Echelon Level	X2	Qualitative	Attribute	3
Rationalization	Person Grade/Personal Level Kerja	X3	Quantitative	Attribute	4
Rationalization	Working Period in Work Unit	X4	Quantitative	Attribute	5
Rationalization	Permanent/Contracted Employment Status	X5	Qualitative	Attribute	6
Rationalization	Gender/ Gender	X6	Qualitative	Attribute	7
Pressure	Number of Children/Family	X7	Quantitative	Category / Nominal	8
Opportunity	Number of Work Unit Mutations	X8	Quantitative	Category / Nominal	9
Opportunity	Number of Position Assignments	X9	Quantitative	Category / Nominal	10
Rationalization	Number of Leave Days	X10	Quantitative	Category / Nominal	11
Rationalization	Number of Sick Days	X11	Quantitative	Category / Nominal	12
Pressure	Last year's Performance Appraisal Nilai	X12	Quantitative	Ratio	13
Pressure	Loan Performance Achievement last year	X13	Quantitative	Ratio	14
Pressure	DPK Performance Achievement last year	X14	Quantitative	Ratio	15
Pressure	Money Into Income Ratio	X15	Quantitative	Ratio	16
Pressure	Total Installment Liability	X16	Quantitative	Ratio	17
Pressure	Maximum Collectability of Liability	X17	Quantitative	Ratio	18
Rationalization	Working Period Job Grade	X18	Quantitative	Attribute	19



Fig. 4. Loan Flow Process

accuracy in making measurements. The rule of thumb used for the Composite Reliability (CR) value is > 0.7 (Ghozali). The formula for this CR is:

$$\rho_c = \frac{(\sum \lambda_i)^2 \text{var}F}{(\sum \lambda_i)^2 \text{var}F + \sum \Theta_{ii}}$$

where,

- λ_i = factor loading
- F = factor variance
- Θ_{ii} = error variance

4 Results and Discussion

The microcredit loan process is started with the Marketing stage and then, it is continued with the Initiative, Decision, and Realization Stage. Eventually, the stage is ended with Monitoring and Repayment as shown in Fig. 4. Each stage of the process mostly requires the involvement of officers (humans). Thus, the potential for operational risk is still high due to intentional negligence. In the Marketing stage, the Microcredit RM would find prospective debtors who would be processed further according to the microcredit stages. The information of the prospective debtors are obtained from the List of Potential Borrowers (Pipelines), Referrals from several appointed partners/bank officers, or referrals from existing customers/institutions. At this stage, the RM is responsible for finding, verifying, and ensuring that the data is per field conditions. Sometimes for some reasons, the RM commits fraud with “Calo” (broker) in order to find prospective debtors using fictitious documents, and the microcredit is still disbursed. Collusion between the RM and the Prospective Debtor (Tempilan/Topengan).

The next stage of the process is Analyzing and Proposing. At this stage, the RM is responsible for inputting the documents and simultaneously performing credit analysis. Several risks that might occur during this stage are engineering/falsifying documents, making errors on data input into the loan application process intentionally, or colluding with the debtor. It is expected that fictitious credit might be exist due to document falsification. Some infrastructure or tools have been implemented to mitigate the risks referred to by the RM such as Geo Tagging, GPS, and re-verification by the RM’s supervisor.

Then, on the approval and Disbursing stage, the manager supervising the RM must make a credit decision regarding debtor eligibility, credit amount, and credit terms. If all the credit requirements have been met, the debtor can disburse and enjoy it. The risk of fraud at this stage can be found on the credit amount. This can happen as the entitled

debtor does not carry out credit disbursement or the credit is not used by the debtor but by another party, either partially (Tempilan credit) or entirely (Topengan credit). Another risk of fraud is gratification by the debtor to the RM officer as an “expression of gratitude.”

The final stage of the process is Monitoring and Repayment. The loan process cycle at the bank is started with marketing and ended with repayment. If there is no repayment process, the credit is in arrears. On the monitoring stage, the RM officer would monitor the business condition of the debtor and ensure that the debtor can pay installments and repay loans. At this stage, the risk of fraud that frequently occurs is that the officer delays the installment payment deposit entrusted to the officer. The officer’s motivation is to use the deposit money for personal purposes. In summary, the stage the microcredit loan process can be seen in Table 2.

Considering the results of the risk identification and risk mitigation process that have been discussed above, the implementation of effective operational risk management is crucial. According to Onyiriuba (2016), fraud was the most disturbing risk among several existing operational risk causes. Mbeba (2007) viewed operational risk as a vulnerability faced by microfinance institutions in their daily activities, including portfolio quality, fraud and theft, data and reporting integration, which can erode the company’s capital and fail its performance targets. According to Wulandari and Natasari (2018) the company implemented a fraud prevention strategy with the following stages; (1) Mapping the sources, areas, and fraud schemes that have occurred and may occur, (2) Identifying fraud risks by area, (3) Mapping the fraud risks in fraud schemes so that a risk register is formed, (4) Performing an assessment related to the occurrence and impact so that a fraud risk map is formed, and (5) Conducting monitoring and evaluation.

Bank ‘X’ had RM to serve micro-loans spread throughout Indonesia. The Data was obtained from 2017 – 2019 with the following rates, RM was 28,385 (2017), 28,136 (2018) and 28,053 (2019) respectively. The employee turnover rate during the aforementioned period was 1 percent. During that period, 72.4 percent of the workers were male, and 27.6 percent were female one. 49.8 percent are married in marital status, while the remaining 50.2 percent are unmarried. The mean age was 32 years, and the predominance of age was in the range of 30–35 years (65 percent). Although Bank X offices are spread across all provinces in Indonesia, 55% were located on the island of Java. The distribution of tenure as Micro RM at bank ‘X’ is six years. Then, the most dominant (40%) were RM workers with 5–7 years of service, and 10% of workers had up to 1 year of service. Referring to bank ‘X’s’ marketing strategy, 97 percent of marketers are marketers for micro-loans for the productive sector, while the rest are in the consumptive sector Table 3.

In terms of the financial capabilities of RM workers, the data reveals that the average RM marketer has at least two bank loan accounts. Meanwhile, most RMs have an outgoing account balance of 3 – 6 times the amount of wages received from bank ‘X’ in terms of out- of-account transactions. Then, most RMs have an incoming transaction of 3 times from the total amount of wages received. The first step in order to analyse using CFA is to determine the red flags of fraud incidents obtained from the RM profile. Identification and selection of red flags that can be used as independent variables are based on the taxonomy of red flags [1], Fraud Detection parameters of each component

of the Fraud triangle theory [15] and the results of discussions with stakeholders of the fraud incident at bank 'X'. The following table lists the red flags used to make variables in determining the components of the Fraud triangle theory.

In the process of data cleansing for missing values and outliers, the following action is done:

a) Missing Value, several techniques were used for the continuous and categorical data to overcome the missing value. The missing values for continuous variables is carried out by imputation based on the median value of the data. While the missing values for categorical variables, imputation is done based on the data mode. Then, the outliers data is carried out by considering the combination of alternative techniques that are commonly used, namely: Outlier data is omitted as it does not reflect the actual distribution of data. Alternatively, the outlier data was obtained due to data collection errors and computer input errors. Then, the Outlier data is retained (retention) and it does not need to be removed. Z-score is calculated to see the distance between the standard deviation and the means. Outlier is set if $|Z| > 3$.

The Fig. 5 below is a path diagram of the Second Order CFA risk of fraud by marketers, which is indicated by each standardized value.

The path diagram above shows that the highest loading factor value is found in opportunity (o). Then, the most significant factor is followed by pressure (p) and rationalization (r). In other words, opportunity (o) significantly influences the risk of fraud committed by a marketer. The following are the details of the path diagram of the Second Order CFA risk of fraud by marketers, Table 4.

After the path diagram is obtained, the stage continues to the model identification. It is carried out before the CFA model estimation stage. The number of parameters to be estimated (t) is 3, while the number of variance and covariance between the manifest variable (s) is 41. It shows that the model is over-identified since the value of $t < s$. Thus, it is necessary to obtain the estimated value of the parameters formed in the CFA model. The estimation used in this research is the Maximum Likelihood Estimation. Then, the Model testing aims to find out the unidimensional indicator variables in explaining the latent variables, with hypotheses and model fit criteria shown in the following Table 5:

Based on the data analysis above, it is found who meet the fit criteria than those who do not. It is indicated by 11 tests that meet the fit criteria, while only two tests do not meet the fitness criteria. The following is the loading factor value from testing the validity of each indicator on the latent variables shown in the Table 6.

The Table 6 reveals that there are 13 significant indicators, specifically the sources that compose the latent risk variable. It is indicated by the p-value of each indicator, which is less than the significant level with $= 0.05$. in contrast, the P1 and P2 are insignificant because they have a p-value $> (0.05)$. Thus, the analysis is continued on first order confirmatory factor analysis (CFA) to ensure that the significant variables are used to measure the fraud risk of marketers. However, it is necessary to test first how much the value of construct reliability (CR) is. The value of construct reliability (CR) second-order risk of fraud by marketers is 0.512, meaning that the risk of fraud by marketers has good reliability.

Table 4. Details of Second Order CFA risk of fraud by marketers

Latent Variables	Indicator	Information	Description
pressure	P1	outstanding_2017_woe	Last year's Performance Achievements
pressure	P2	ratio_dpk_2017_woe	DPK Performance Achievement last year
pressure	P3	amount_payment_mantri_woe	Total Installment Liability
pressure	P4	max_term_mantri_woe	Maximum Collectability of Liability
pressure	P5	ECHELON	Echelon Level
pressure	P6	ratio_credit_income_woe	Cash into income ratio
pressure	P7	AGE_woe	Age
pressure	P8	THE NUMBER OF DEPENDENTS	Number of Children/family
Opportunity	O1	MKPG	Person Grade Work Period
Opportunity	O2	MKU_woe	Working Period in Work Unit
Opportunity	O3	Move_Uker_woe	Number of Work Unit Mutations
Opportunity	O4	Number_Assignments_woe	Number of Position Assignments
Opportunity	O5	MKE_woe	Effective Working Time
Opportunity	O6	Leave_Annual_woe	Number of Leave Days
Opportunity	O7	SMK_2017_woe	Last Year's Performance Achievements
Opportunity	O8	STATUSADJ	Marital status
Opportunity	O9	Permission_Pain_woe	Number of sick days
Opportunity	O10	MKJG_woe	Working Period Job Grade
rationalization	R1	JG	Job Grade Level Position
rationalization	R2	ESGDESC	Permanent/Contracted Employment Status
rationalization	R3	GENDER17	Gender/Gender
rationalization	R4	TW_III	Last year's Performance Appraisal Nilai
rationalization	R5	LAST EDUCATION	Last education

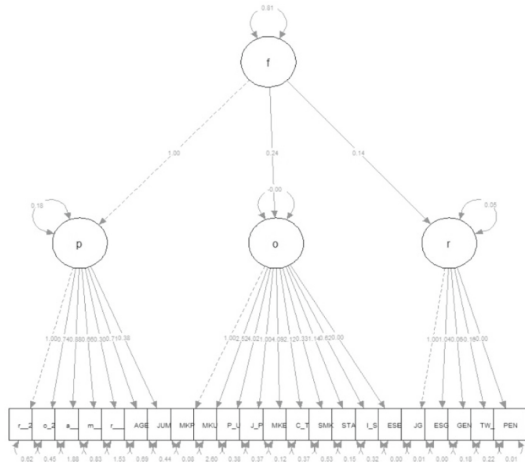


Fig. 5. Path diagram of Second Order CFA risk of fraud by marketers

Table 5. Model Test Results

No	Statistics	The calculation results	Criteria	Information
1	Minimum fit function chi-square (χ^2)	221.882 (p_value=0.0)	p_value > 5%	unwell
2	RMSEA	0.07	< 0.08	fit
3	RMR	0.04	<= 0.1	fit
4	SRMR	0.04	<= 0.1	fit
5	GFI	1.0	>= 0.9	fit
6	AGFI	1.0	>= 0.9	fit
7	NFI	0.9	>= 0.9	fit
8	NNFI	0.9	>= 0.9	fit
9	CFI	0.9	>= 0.9	fit
10	IFI	0.9	>= 0.9	fit
11	RFI	0.9	>= 0.9	fit
12	PNFI	0.8	>= 0.9	unwell

Table 6. The loading factor value from testing the validity of each indicator on the latent variable

Latent Variables	Indicator	Estimate	Std.Err	z- value	P(> z)
pressure	P1	0.6	0.0	72.4	0.0
pressure	P2	0.4	0.0	77.9	0.0
pressure	P3	1.9	0.0	94.3	0.0
pressure	P4	0.8	0.0	92.5	0.0
pressure	P5	1.5	0.0	100.6	0.0
pressure	P6	0.7	0.0	90.9	0.0
pressure	P7	0.5	0.0	96.3	0.0
pressure	P8	0.0	0.0	80.2	0.0
Opportunity	O1	2.6	0.0	101.6	0.0
Opportunity	O2	0.7	0.0	101.3	0.0
Opportunity	O3	0.4	0.0	101.5	0.0
Opportunity	O4	0.4	0.0	100.7	0.0
Opportunity	O5	0.4	0.0	101.4	0.0
Opportunity	O6	0.5	0.0	101.5	0.0
Opportunity	O7	0.2	0.0	101.6	0.0
Opportunity	O8	0.3	0.0	101.5	0.0
Opportunity	O9	0.0	0.0	101.5	0.0
Opportunity	O10	0.0	0.0	-2.4	0.0
rationalization	R1	0.0	0.0	33.0	0.0

5 Conclusion

Fraud is one of the most influential factors in society. Because of fraud, several companies are experiencing financial problems and threatening business continuity. The fraud incidence in the business tends to increase, regardless of the size and profitability of the company. The Internal fraud is a significant and growing problem. In line with the company's automation process, the opportunity to commit fraud also widens. Thus, fraud prevention and detection efforts are increasingly problematic. The fraud incidence in the microloan process was caused by rationalization factors based on the analysis Using the CFA method and research variables using red flags from the RM profile. Besides, the path diagram of the Second Order CFA risk of fraud by marketers (RM) revealed that the most significant loading factor value is rationalization. Then, it was followed by pressure and opportunity factors. In other words, rationalization significantly influences the risk of fraud committed by an RM employee. [25] concluded that rationalization has a positive and significant relationship to fraud (asset misappropriation). It means that the ability and behavior of individuals in the bank can influence someone to justify fraudulent behavior.

Based on the results of the research above, some recommendations are proposed. For instance, the bank is suggested to put its focus more on matters related to rationalization, especially the redflags that are part of rationalization component. Meanwhile, the limit of this research is that the CFA method used is part of the process of making a risk event prediction model using Machine Learning (ML) XGBoost, as a tool to increase the effectiveness of the implementation of Governance, Risk, and Compliance in banks that serve microloans. Then, the author suggests further research on the CFA's conclusions as it is essential to create a fraud prediction model.

References

1. D. Mangala, P. Kumari. 2015. Corporate Fraud prevention and detection: revisiting the Literature. *Journal of Commerce & Accounting Research* Volume 4 Issue 1 January 2015
2. JD. Hansen, TA. Buckhoff. 2000. To catch a thief. *Journal of Accountancy*. Vol. 189. Iss. 3. pp. 43-46
3. KHS. Pickett. 2012. *Fraud Smart*. John Wiley and Sons, Ltd., Chichester. The UK.
4. Ramamoorti, S. and W. Olsen. 2007. *Fraud: The Human Factor*. *Financial Executives*. July/August 2007. 23; 6.
5. M. Omar, A. Nawawi, ASA Puteh Salin, 2016. The causes, impact, and prevention of employee fraud. *Journal of Financial Crime*. Vol. 23, Iss 4, 2016. pp 1012- 1027
6. S. Padgett. 2015. *Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud*. John Wiley and Sons Inc. New Jersey
7. Baz, Rm, Samsudin Hospital, AB Che-ahmad, OMJ Popula. 2016. Capability Component of Fraud and Fraud Prevention in the Saudi Arabian Banking Sector. *International Journal of Economics and Financial Issues*. 2016, 6 (S4) 68–71
8. MK. Kapardis, K. Papastergiou. 2016. Fraud victimization in Greece: room for improvement in prevention and detection. *Journal of Financial Crime* Vol. 23 No. 2, 2016 pp. 481–500
9. N. Lambe. 2013. Profile of Fraudster Lessons for those Charged with Governance. *Accounting Ireland*. December 2013. Vol. 45 No. 6
10. TRH. Meliana. 2019. *Indonesian Banking Fraud*. *Exploration Studies. Proceedings of the 2nd National Expert Seminar in 2019*. Book 2: Social and Humanities
11. Z. Haithem, KD. Ayisi, K. El-Hedhli, 2014. Consumer Fraudulent Behavior: A Cross-Cultural Perspective. *Proceedings of ASBBS*. Vol. 21 Number 1. February 2014
12. S. Ramamoorti, W. Olsen. 2007. *Fraud: The Human Factor*. *Financial Executives*. July/ August 2007. 23; 6.
13. HD. Glover, JY. Aono. 1995. Changing the model for the prevention and detection of fraud. *Managerial Auditing Journal*, Vol. 10 No. 5, 1995, pp. 3–9
14. ZN. Mohd-Sanusi, N. Mohamed, Omar, MD Mohd-Nassir, 2015. Effects of Internal controls, Fraud Motives, and Experience in Assessing Likelihood of Fraud Risk. *Journal of Economics, Business and Management*, Vol. 3, No. 2, February 2015
15. M. Hollow. 2014. Money, morals, and motives: An exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime*, Vol. 21 Issue: 2, pp.174-190
16. W. Albrecht. 2014. Who Commits Fraud and Why. *Journal of Financial Crime*, Vol. 21 Issue 2, pp. 174-190
17. A. Nawawi, ASA. Puteh Salin. 2018. Employee Fraud and Misconduct: Empirical Evidence from a Telecommunication Company. *Information and Computer Security* Vol.26No.1 2018 pp. 129–144

17. JB. Suh, R. Nicolaidis, R. Trafford. 2019. The effects of reducing opportunity and Fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime, and Justice*. 56 (2019) 79–88
18. F. Zamzami, ND Nusa, RP. Timur, 2016. The Effectiveness of Fraud Prevention and Detection Methods at Universities in Indonesia. *International Journal of Economics and Financial Issues*. Vol. 6. Special Issue (S3) 66-69
19. MA. Tiggos. 2002. Why Fraud management is unstoppable. *The CPA Journal*. Dec 2002. Vol. 72. Iss. 12. pp. 34-41.
20. Butler, Nicholas. 2009. Addressing and Mitigating the Risks of Fraud. *The Secured Lenders*; Mar/Apr 2007; 63, 2; pg. 70
21. S. Owusu-Ansah, GD Moyes, PB Oyelere, D. Hay. 2002. An empirical analysis of the likelihood of detecting Fraud in New Zealand", *Managerial Auditing Journal*, Vol. 17 Issue: 4, pp. 192-204
22. OIH. Arvid, C. Birnbrich, 2012. The impact of Fraud prevention on bank-customer relationships. *The International Journal of Bank Marketing*. Vol. 30, Iss. 5, (2012): pp. 390–407.
23. M. Hibino, M. Sharifi. 2013. Fraud Prevention Methodology: The Ishikawa Diagram. *Internal Auditing*. Vol. 28. Iss 5. (Sept/ Oct 2013). pp. 27–36
24. R. Hartugi. 2007. Understanding the success factors of micro-finance institutions in a developing country. *International Journal of Social Economics* Vol. 34 No. 6, 2007 pp. 388–401
25. Kazemian, S., J. Said, EH Nia, and H Vakilifard. 2019. Examining fraud risk factors on asset misappropriation: evidence from the Iranian banking industry. *Journal of Financial Crime* Vol. 26 No. 2, 2019 pp. 447–463

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

