PAPER – OPEN ACCESS

Analysis of Operational Risk Mitigation in Customer Identification Files (CIF) Management at PT. Bank SUMUT

Author : Heru Dian Herlambang, et al
DOI : 10.32734/lwsa.v9i2.2798
Electronic ISSN : 2654-7066
Print ISSN : 2654-7058

Volume 9 Issue 2 – 2026 TALENTA Conference Series: Local Wisdom, Social, and Arts (LWSA)

LWSA Conference Series 09 (2026)
TALENTA Conference Series
Available online at https://talentaconfseries.usu.ac.id

Analysis of Operational Risk Mitigation in Customer Identification Files (CIF) Management at PT. Bank SUMUT

Heru Dian Herlambang[1], Rulianda Purnomo Wibowo[2], Nazaruddin[3]

[1]*Post Graduate Student Student Manajemen, Universitas Sumatera Utara*
[2]*Faculty of Agriculture Universitas Sumatera Utara*
[3]*Faculty of Engineering, Universitas Sumatera Utara*

ubebryant@gmail.com, rulianda_wibowo@usu.ac.id, nazarmtd60@gmail.com

Abstrak

Penelitian ini mengkaji mitigasi risiko operasional pada proses Customer Identification File (CIF) di PT Bank Sumut dengan menerapkan metode Failure Mode and Effect Analysis (FMEA) dan Fault Tree Analysis (FTA). Tujuan utama penelitian adalah mengidentifikasi kondisi kritis yang memicu kegagalan proses CIF serta merancang rekomendasi mitigasi yang tepat. Metode FMEA diaplikasikan untuk menentukan Severity (S), Occurrence (O), dan Detection (D) pada beberapa failure mode, menghasilkan Risk Priority Number (RPN) tertinggi pada kegagalan pemindaian identitas nasabah (RPN=50) dan pengisian data ambigu (RPN=48). Selanjutnya, FTA memetakan akar penyebab kegagalan tersebut ke dalam dua kategori utama: human error (kurangnya pemahaman SOP dan pelatihan staf) serta system failure (sinkronisasi batch-based antara CBS dan ARS, dan antarmuka modul yang kurang intuitif). Hasil analisis menunjukkan bahwa kelemahan paling mendasar terletak pada pemahaman karyawan terhadap prosedur serta minimnya validasi otomatis dalam sistem, sedangkan deteksi dini masih lemah (D=4–5) sehingga sering kali kegagalan hanya terungkap saat audit. Berdasarkan temuan ini, penelitian merekomendasikan perbaikan SOP, pelatihan berkala, implementasi real-time synchronization, dan mekanisme validasi otomatis untuk menurunkan RPN, memperkuat kepatuhan regulasi, dan meningkatkan kualitas data nasabah

Kata Kunci: Kesalahan Personel; FMEA; Fault Tree Analysis; Akurasi Data; Proses CIF

Abstract

This study examines the mitigation of operational risks in the Customer Identification File (CIF) process at PT Bank Sumut by applying the Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) methods. The objective of the research is to identify critical conditions that trigger failures in the CIF process and to design appropriate mitigation recommendations. The FMEA method was applied to determine Severity (S), Occurrence (O), and Detection (D) on several failure modes, resulting in the highest Risk Priority Number (RPN) for the failure of customer identity scanning (RPN=50) and ambiguous data entry (RPN=48). Next, FTA mapped the root causes of these failures into two main categories: human error (lack of understanding of SOP and staff training) and system failure (batch-based synchronization between CBS and ARS, and a less intuitive module interface). The analysis results indicate that the most fundamental weaknesses lie in employees' understanding of procedures and the lack of automated validation in the system, while early detection remains weak (D=4–5), often resulting in failures being revealed only during audits. Based on these findings, the research recommends improving SOPs, conducting periodic training, implementing real-time synchronization, and establishing automatic validation mechanisms to reduce RPN, strengthen regulatory compliance, and enhance the quality of customer data

Keywords: Human Error; FMEA; Fault Tree Analysis; Data Accuracy; CIF Process

1. Introduction

The banking sector operates in a highly regulated environment where accurate customer data management is critical to ensuring compliance, operational efficiency, and risk mitigation. One of the core components in this process is the Customer Identification File (CIF), a centralized database that stores essential customer information for identity verification, transaction monitoring, and regulatory reporting. CIF is a digital file that contains personal and financial data of bank customers. CIF is a very important database for banks that serves as a unique identity for customers with the following provisions. Each customer is only allowed to

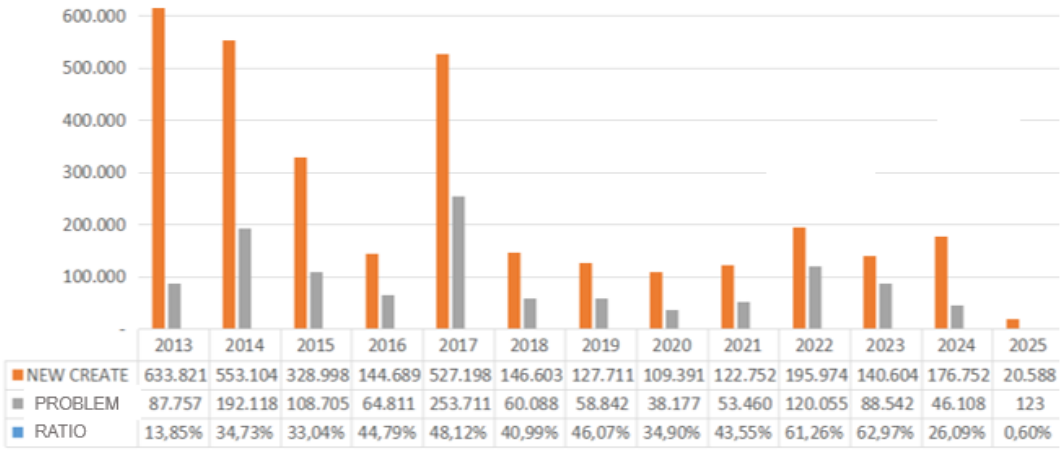
Selection and peer-review under responsibility of The 2nd International Joint Conference on Digitalisation of Sustainable Social Sciences (IJCDSS) 2025
p-ISSN: et al, e-ISSN: 2654-7058, DOI: 10.32734/lwsa.v9i2.2798

have one CIF number at one bank. Customers who have a bank account that is a joint account (account owned by 2 or more people) will be given a different CIF number. The personal data of customers stored in the bank through the customer's CIF is confidential and must not be disclosed. In addition to the usefulness of CIF data for the bank's business, CIF data is also used in reporting activities, requiring a reliable CIF database to ensure reporting accuracy.

In accordance with POJK No. 8 of 2023 article 69 paragraph (3), "Financial Services Companies are required to have and maintain a unified customer profile (single customer identification file), at least the information as referred to in Article 25 and Article 28 paragraph (1)." However, errors in CIF management—such as inaccurate data entry, duplicate records, or non-compliance with regulatory standards—can lead to severe consequences, including financial losses, legal penalties, and reputational damage. Errors in the data input process within the banking system not only affect the quality of service and internal operations but also have the potential to cause serious legal consequences. Pramudita (2024) emphasizes that errors in reporting data to the Financial Information Service System (SLIK) can result in sanctions such as the freezing of business activities, a decline in the bank's health rating, and administrative penalties from regulatory authorities. Additionally, these violations also affect the assessment of compliance and the bank's ability to perform its intermediation function in a healthy manner. Meanwhile,Cardoso and Cardoso (2024) show that negligence in reporting that impacts customer losses can lead to legal liability for the bank. This indicates that the accuracy and precision of data in the banking system are a legal obligation, not merely an administrative procedure. Therefore, every data input process must be carried out with high caution and strict supervision to avoid legal risks that could harm the reputation and sustainability of banking institutions.

Based on previous studies, it appears that the main sources of operational risk in the banking sector stem from human factors and weaknesses in internal processes. Meshcheriakov et al. (2024) emphasize that human factors are the most unpredictable yet have a significant impact on the operational stability of banks. This view is reinforced by the research of (Okeke, Aganoke, and Onuorah 2018), which shows that risks from internal processes and the use of technology significantly reduce the performance of banking organizations, while external risks have only a weak influence. Berger et al. (2018) even link this operational risk to broader systemic risks, which can trigger a crisis if not managed properly. Considering the results of the four studies, it becomes clear that controlling operational risks, particularly those stemming from human errors and process failures, is not only important but also urgent to address. Structured risk control will help organizations prevent the escalation of operational disruptions into systemic threats, as well as maintain the sustainability and resilience of financial institutions amidst the complexities of the modern work environment.

PT. Bank SUMUT, a regional bank in Indonesia, faces significant challenges in maintaining the integrity of its CIF database. These errors stem from multiple factors, including human oversight, inadequate procedures, technological limitations, and external pressures. Without effective mitigation strategies, these issues expose the bank to regulatory sanctions, operational disruptions, and diminished customer trust. The graph of the CIF Problematic Ratio per Year is as follows.



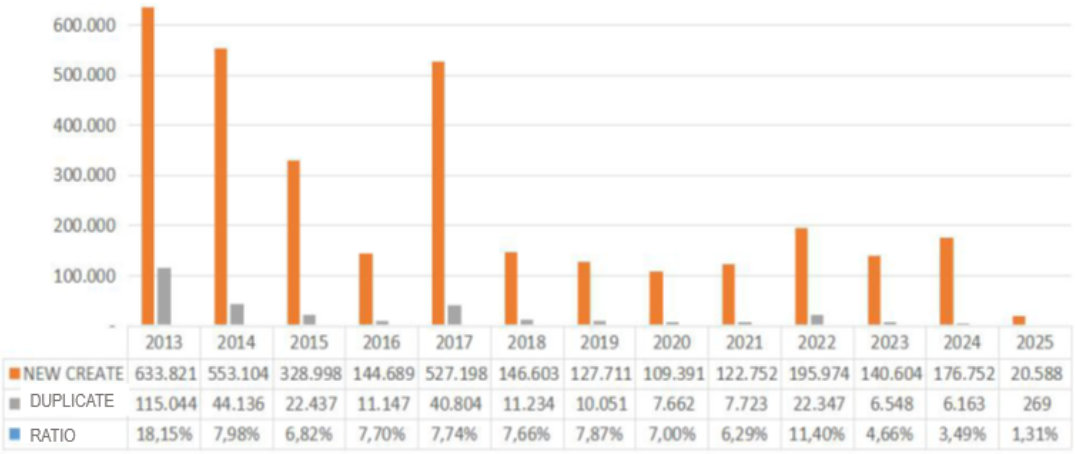
	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NEW CREATE	633.821	553.104	328.998	144.689	527.198	146.603	127.711	109.391	122.752	195.974	140.604	176.752	20.588
PROBLEM	87.757	192.118	108.705	64.811	253.711	60.088	58.842	38.177	53.460	120.055	88.542	46.108	123
RATIO	13,85%	34,73%	33,04%	44,79%	48,12%	40,99%	46,07%	34,90%	43,55%	61,26%	62,97%	26,09%	0,60%

Figure 1. Problematic CIF Ratio Graph (Year)

Based on figure 1 show the problematic CIF ratui, which is CIF that does not comply with the standardization of data entry customers). The figure 1 show that the average error in filling out the CIF database of Bank SUMUT is 90,192 CIF or 37.77% per year from New CIF.

The data show that, while the number of newly created CIF records has fluctuated significantly from 2013 to 2025, the proportion of problematic CIF entries has often remained high. For instance, in 2017 the bank recorded 527,198 new CIFs, of which 253,711—or 48.12%—were problematic. Similarly, in 2022 and 2023 the proportion of problematic CIFs reached 61.26% and 62.97%, respectively, indicating substantial weaknesses in both procedural compliance and system reliability.

Such high error ratios reveal that ensuring data accuracy is not merely a technical process but also an organizational challenge that involves human resources, operational procedures, and technological infrastructure. The persistence of problematic CIF entries suggests that lapses in staff training, inadequate enforcement of Standard Operating Procedures (SOPs), and system limitations continue to undermine data quality. This directly threatens the integrity of the CIF database, as duplicate, inconsistent, or incomplete records compromise regulatory compliance, increase operational risks, and erode customer trust.



	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
NEW CREATE	633.821	553.104	328.998	144.689	527.198	146.603	127.711	109.391	122.752	195.974	140.604	176.752	20.588
DUPLICATE	115.044	44.136	22.437	11.147	40.804	11.234	10.051	7.662	7.723	22.347	6.548	6.163	269
RATIO	18,15%	7,98%	6,82%	7,70%	7,74%	7,66%	7,87%	7,00%	6,29%	11,40%	4,66%	3,49%	1,31%

Figure 2. Double CIF Ratio Graph (Year)

Figure 2 illustrates the trend of newly created CIF records, duplicate entries, and their corresponding ratios from 2013 to 2025. The data reveal a substantial decline in the number of new CIFs from 633,821 in 2013 to only 20,588 in 2025, accompanied by a significant reduction in duplicate cases from 115,044 (18.15%) in 2013 to merely 269 (1.31%) in 2025. Despite occasional fluctuations, the overall trend indicates a consistent improvement in data quality and accuracy, as reflected in the steady decrease of the duplication ratio over the observed period. Although the overall trend indicates improvement, the data also reveal fluctuations in specific years. For instance, the duplication ratio remained relatively high at 11.40% in 2021, before declining again in subsequent years. Such irregularities may reflect temporary lapses in procedural compliance, system upgrades, or the integration of new regulatory requirements that momentarily affected data accuracy. Nevertheless, the long-term downward trend in duplication ratios demonstrates that corrective measures, including enhanced staff training, refinement of standard operating procedures (SOPs), and system improvements, have effectively addressed most of the recurring problems.

The analysis of both figures highlights the persistent challenges faced by PT. Bank SUMUT in maintaining the accuracy and integrity of its Customer Identification File (CIF) database. Despite fluctuations in the number of newly created CIFs, the proportion of duplicate and problematic records remained considerably high across several years, with error ratios exceeding 40% in some periods and even reaching above 60% in 2022 and 2023. Such conditions clearly demonstrate systemic weaknesses in data entry procedures, staff adherence to Standard Operating Procedures (SOPs), and technological infrastructure.

These findings underscore that the CIF issue is not an isolated administrative problem but a critical operational risk that threatens regulatory compliance, financial stability, and customer trust. Addressing this challenge requires not only technical interventions—such as real-time synchronization, automated validation, and enhanced database management—but also organizational measures, including periodic training, stronger internal controls, and continuous risk monitoring.

Therefore, raising this issue is highly relevant and urgent, as it allows for a comprehensive investigation into the root causes of CIF errors. By identifying and understanding these root causes, the bank can design effective mitigation strategies to improve data accuracy, reduce operational risks, and strengthen institutional resilience. Ultimately, prioritizing CIF improvements is essential for safeguarding the bank's reputation, ensuring sustainable operations, and reinforcing public trust in the banking sector.

The issue with the CIF database has resulted in Regulatory sanctions from the Financial Services Authority (OJK) to Bank SUMUT, financial losses, and reduced customer trust. Therefore, it is important to reduce CIF operational risks in order to reduce the impact of these risks on CIF database activities at PT. Bank SUMUT. This issue matters because inaccuracies and errors in the

CIF database can have widespread and serious consequences for the bank, including regulatory compliance risks, operational disruptions, financial losses, reputational damage, risk management and mitigation importance.

Overall, guaranteeing data accuracy in CIF is critical for maintaining legal compliance, operational stability, financial integrity, and public trust, making this issue highly significant for the bank's health and reputation. This issue impacts to the bank's operational efficiency, legal compliance, customer satisfaction, and overall reputation, affecting a broad spectrum of internal and external stakeholders.

Ensuring data accuracy in Customer Identification Files (CIF) is essential for maintaining regulatory compliance, operational stability, financial integrity, and public trust. This study aims to strengthen CIF management at PT. Bank SUMUT by systematically identifying and mitigating operational risks through the application of Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) (DeGroff and Hou (2025). Specifically, the research seeks to identify the root causes of data inaccuracies and to develop comprehensive mitigation strategies that not only reduce CIF-related errors but also enhance regulatory compliance, improve operational resilience, and safeguard institutional reputation. In doing so, this study contributes to the academic discourse on operational risk management while providing practical insights for the advancement of sustainable banking practices.

This research will provide actionable recommendations to enhance CIF accuracy, streamline compliance processes, and strengthen the bank's operational resilience. By integrating FMEA and FTA, this study not only contributes to academic discourse on operational risk management but also offers practical value for PT. Bank SUMUT and similar banking institutions facing analogous challenges. Ultimately, the goal is to reduce CIF-related errors, align with regulatory requirements, and foster sustainable banking operations.

2. Literature Review

According to AS/NZS Standard 4360:1995, risk is the chance of something happening, that has an impact on objectives measured in terms of consequences and probability. Which Companies that implement risk assessment will become more aware and prepared facing the possibility of potential risks occurring and can predicting the handling scenarios. Risk management in organizations is a system for managing risks comprehensively. faced by the organization comprehensively to enhance value company (Hanafi, 2006). Uncertainty is a state of mind filled with doubt. By therefore, risk management is carried out by the company to realize business processes that is optimal and provides benefits for the company and society (Rosih, Choiri, and Yuniarti 2015)

Risk is the opportunity for adverse events to occur that caused by the uncertainty of what will be faced. Uncertainty is a potential change that will occur in the future as the consequence of the inability to know what will happen if an activity activity is carried out at the moment. The starting point in risk management is the placement uncertainty (Sari, Siregar, and Harahap 2020). According to Vaughan (1978) in (Rosih et al. 2015), there are several definitions of risk, including (a) risk is the chance of loss ; (b) risk is the possibility of loss; (c) risk is uncertainty.

Risk Management in Banking is a systematic process that carried out by banking institutions to identify, measure, monitor, and controlling the risks arising from all banking business activities (Andrianto, Fatihudin, D; Frimansyah. 2019) define bank risk management as a series methodological activities and procedures used to identify, measure, monitor and control risks arising from all banking business activities The main objective of risk management is to minimize potential losses and maximize profits for the Bank. Nurapiah (2019) mentions that risk management is a process of anticipating risks to prevent losses does not occur to the organization.

Operational risk in banking is the potential for losses that caused by failures in internal processes, human errors, or systems that inadequate. This risk can arise from various sources, such as errors in transaction processing, internal or external fraud, technology system failure information, as well as external events such as natural disasters or cybersecurity breaches. Basel Committee on Banking Supervision defines operational risk as risk of loss or inadequacy arising from internal processes, human factors, and system, or from external events.

Sutrisno et al. (2023) mention that operational risk is the risk resulting from the lack of information systems or internal control systems that will resulting in unexpected losses. Ristanović, Primorac, and Kozina (2021) mentioned that operational risk in banking is a potential risk that is quite difficult predicted and have the greatest impact on the sustainability of the industry banking. Mulyati (2018) mentions that the implementation of risk management, including operational risks related to HR, processes, and systems in controlling controlling credit risk. Fahmy (2020) and Sutrisno et al. (2023) mention that operational risk is the largest risk in banking, which is quite complex and difficult to predict. Recent research by Testa et al. (2024) found that the significant role of employee training in enhancing bank stability, he also mentioned that improving the soft skills of bank employees can reduce bank credit risk. Vasiliev et al., (2018) mention that banking activities require a healthy risk management culture and operational risk are categories of risk main in banking. According to Nurapiah (2019), it is mentioned that the risk losses caused by inadequate internal processes, process failures internal, human error, system failure, and/or external events external factors that affect the Bank's operations. Based on Hull (2018), measuring operational risk is much more difficult than measuring credit risk

or market risk. Financial institutions consciously take market and credit risk, and many traded instruments that can be used to reduce this risk. However, on the contrary, operational risk is a component important part of business operations. Managers must identify what types of risks need to be taken and insured is an important part of operational risk management. Taking operational risks that were not even recognized as risks before always has the potential to cause significant losses.

The impact of operational risk on banking can be very significant. In addition to direct financial losses, operational risks can also damage the bank's reputation, reducing customer trust, and even threatening business continuity. Therefore, operational risk management becomes very important for every banking institution to manage operational risk, banks need to implement a system strong internal controls, conduct risk identification and assessment periodically, and developing a comprehensive risk mitigation plan.

Operational risk in banking encompasses various types that can threatens the stability and performance of a financial institution. Operational risk based on the document from BCBS titled *International Convergence of Capital Measurement and Capital Standards (A Revised Framework, June 2004), states that "Operasional risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*(Andrew Cornford 2005; BSTDB 2014; Fahmy 2020) categorize operational risk operational into two main groups.

First, internal factor, p***eople risk.*** This risk is related to the actions or negligence of individuals within the organization, that can cause losses. Human resource management and employee behavior can be a significant source of operational risk. Employees less trained or overworked employees can inadvertently expose the Bank to operational risk (for example, through errors processing). Understanding the mandate, trust, and respect towards institutions and adherence to the policies and strategies of the World Bank are key to the effective use of human resources. In addition, sustainable employee availability, or the Bank's ability to replace them, can affect the Bank's ability to recover from disruption to its operational continuity. Therefore, the Bank can achieve significant improvements in operational risk control and reduce exposure if the Bank invests time and money to creating the right risk culture, where employees are aware of the risks operational and encouraged to learn from their mistakes. Coleman (2011) deliberate behavior such as fraud or malicious damage. Errors can arise from factors such as fatigue, inability, lack of management oversight, and inadequate staff numbers. Knežević (2013) states that the most important operational risk factor, based on the number of incidents risk, is human error with a total of 54%. Examples of human risks include: a) Human error: Mistakes in data input, calculations, or decision-making; b) Lack of competence: Employees do not have sufficient knowledge or sufficient skills to perform their duties; c) Fraud: Actions taken by employees to gain unlawful personal gain; d) Collusion: The involvement of a group of people in actions that harmful to the Bank.

Process Risk, related to deficiencies or weaknesses in the business process that can cause losses. Many systems and processes support operations Bank, such as information technology systems, human resource management systems, credit risk management system, market, insurance and liquidity, and even the system operational risk management. The Bank's credit risk management system, for example, must involve the processes of identification, measurement, monitoring, and assessment.

Complex or poorly designed systems and processes can lead to operational losses, such as not meeting goals or malfunctioning. As a result, the Bank may face various issues, such as errors processing, fraud, and data security breaches. In addition, system automation that are larger and our dependence on information technology might change the danger from small manual processing errors to systematic errors systematic. Examples of process risks include: a) Deficiencies in procedures: Procedures that are unclear, inefficient, or incomplete; b) failure to follow procedures: Employees do not follow the established procedures; c)Lack of supervision: The absence of adequate oversight of the implementation of business processes; d)Failure to identify and manage risks: Failure to identifying and measuring existing risks.

Last in internal factor is Systems Risk This risk is related to the failure or inadequacy of the technology system information used by the Bank. Examples of system risks include: a) Software failure: Errors in the computer system that cause disruption in banking services; b) Hardware failure: Damage to servers, networks, or other devices other hardware that disrupts the Bank's operations; c) Communication failure: Disruption in the communication network that causing the banking services to be interrupted; d)Failure in data management: Data loss, data corruption, or unauthorized access unauthorized access to data.

Second, External Factors, the events can have a significant impact on the company. The bank must realize that expected and unexpected changes in its operations can become a major source of operational risk. The bank must have appropriate arrangements, considering the nature, scale, and the complexity of its business, to ensure that the Bank can continue to operate and fulfill its regulatory obligations in the event of an unexpected disruption. This arrangement must be updated and tested periodically to ensure effectiveness. Disturbing events The events include fires, floods, earthquakes earth, terrorist actions, vandalism, power outages, etc. The bank must assess the potential the risk of such an event occurring, designing and implementing systems and disaster recovery procedures, with the aim of ensuring continuity activities. Regarding the monetary losses caused by the event, the bank must evaluate potential costs and obtain the appropriate insurance. Use of Consultants and Outsourcing Services Outsourcing arrangements require careful management to provide benefits, and if it not managed adequately, the level of operational risk faced by the Bank may increase, as well as the use and dependence that excessive. for the use of consultants for activities that might be more effective developed internally. Specifically, the issue that has become concern is the loss of control over the process. This can pose serious threat to the continuity of its operations if the service provider experiencing failure.

Analysis of operational risks in various sectors shows that the sources of risk do not only come from technical factors but also from human aspects and internal processes. A study by (Rosih et al. 2015) used the Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) approaches to identify critical risks in the Logistics Department, which include inventory management, warehouse supervision, spare parts circulation, administration, and human resource management. These five main risks are deemed to require immediate attention to prevent broader operational losses. Cahyabuana (2018) states that FMEA provides consistent assessment results in identifying banking operational risks. Pangestuti, Nastiti, and Husniaty (2021) also explains that FMEA can identify internal and external risks in financial companies during the COVID pandemic.

According to McDermott, Mikulak (2008), one of the methods often used to identify risk-causing components and prevent issues it occurs is by using the Failure Mode and Effect Analysis (FMEA) method. According to (Rosih et al. 2015) to identify critical risks and the process operational risk management can use the Failure Mode and Effect method Analysis (FMEA) and Fault Tree Analysis (FTA) methods. Failure Mode and Effect Analysis (FMEA) is a commonly used method to identify and eliminate failures, problems, errors, and so on from systems, designs, processes, and/or services before reaching the customer (Ierace 2010). Attention The main focus of FMEA is to proactively assess the risk of potential failure modes. so that appropriate corrective actions can be taken before the failure occurs. Fault Tree Analysis (FTA) is a deductive technique used to model system failure by starting from the undesired outcome (failure) and working backward to find the cause. The tree that is built serves to show cause-and-effect relationships and can be used to evaluate risks and potential failures in the system.

Based on theoretical foundation, problem formulation, research objectives, review of previous research previously, the conceptual framework in this research can be seen in below:

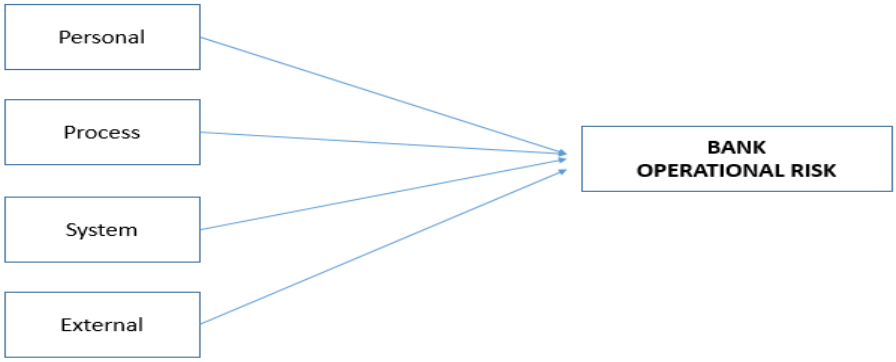


Figure 3. Conceptual Framework

Based on Figure 3, this research highlights four main sources of operational risk in the management of Customer Identification Files (CIF) at PT. Bank SUMUT, namely: personnel, processes, systems, and external factors. These four elements are assumed to be the main contributors to the emergence of banking operational risks, particularly in the context of managing critical customer data. These four factors are assumed to interact with each other and contribute to banking operational risk, so in the context of this research, their interrelationship with CIF management will be analyzed. This conceptual framework serves as the basis for formulating a comprehensive mitigation strategy, through root cause mapping and systematic risk assessment using methods such as Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA). With a comprehensive understanding of the sources of these risks, Bank SUMUT can formulate appropriate preventive and corrective measures to enhance the reliability of operational systems and compliance with regulations.

3. Methods

This research uses a mixed-methods approach that combines qualitative and quantitative methods into a single unit. Conceptually, the research design is systematically and sequentially structured based on the research objectives, starting from problem identification, data collection, analysis, to the formulation of mitigation strategies. For primary data, the researchers conducted survey with questioner's distribution to operational personnel, customer service staff, and management to gain an understanding of the processes and challenges faced, observed the procedures for recording and processing CIF data directly, and reviewed supporting documents such as work records, reports, and operational data. Meanwhile, secondary data were obtained from literature reviews—including scientific articles, journals, and reports related to operational risks and risk management practices—to complement and enrich the analysis. With this design, the research aims to produce a comprehensive overview of risk factors and formulate appropriate mitigation strategies for CIF management in the banking environment.

Data analysis was conducted using the Failure Mode and Effect Analysis (FMEA) method. Analysis (FMEA) and Fault Tree Analysis (FTA) methods. Failure Mode and Effect Analysis (FMEA**),** used to systematically identify potential failure modes in the process of recording CIF, evaluate their effects, and calculate the Risk Priority Number (RPN) to determine which failures are critical and need prioritized mitigation. Fault Tree Analysis (FTA), employed to analyze the root causes of identified failures by constructing a logical model that traces back from an undesired event (e.g., data error) to its basic causes. This top-down approach helps in understanding complex cause-effect relationships and designing effective mitigation strategies

Risk indicators are compiled through the breakdown of each risk variable based on the operational activities of that variable can be seen in Table 1. Operational Variable and Indicator,

Table 1. Operational Variable and Indicator

No	**Variable**	**Indicator**
1	People/ Personal Risk	Administration Activity
		HR Management
2	Process Risk	Regulatory/ Procedure
		Database storage and validation
3	System Risk	Use of Technology
		Technology Development
4	Exsternal Risk	*Force Majeure*
		Relations with Third Parties

The FMEA analysis begins with creating a Failure Mode and Effect Table for each risk indicator to analyze the possible causes and effects of each failure. At this stage, the analysis is conducted by assessing the Severity, Occurrence, and Detection (SOD) values for each risk indicator to obtain the Risk Priority Number (RPN). The measurement of the severity, occurrence, and detection values is as follows.

Table 2. Saverity Score

Score	**Criteria**	**Caracteristic**
1	*Negligible severity*	Negligible negative influence
2	*Mild severity*	The consequences are still mild..
3	*Moderate severity*	The consequences can be felt with a decrease in quality, but it is still within tolerable limits.
4	*High severity*	Decline in quality that is beyond the tolerance limit.
5	*Potential severity*	The consequences that arise have a significant impact on other qualities.

Table 3. Occurance Score

Rating	**Criteria**	**CIF Vs New CIF Error Ratio**
1	Very Low	0 %
2	Low	1% s/d 5 %
3	Moderate	6% s/d 15%
4	High	16% s/d 50%
5	Very High	> 50%

Table 4. Detection Score

Rating	**Criteria**	**Caracteristic**
1	*Very High*	91% to 100% of staff are able to detect errors and function properly
2	*High*	71% to 90% of staff are able to detect errors and function properly
3	*Moderate*	51% to 70% of staff are able to detect errors and most of them function well
4	*Low*	< 50% of staff are able to detect errors and a small portion function well
5	*Impossible*	There is no staff capable of detecting an error

4. Result and Discussions

In this section, the results of the research data processing will be presented, including an overview of the respondents' characteristics such as gender, education level, age, and length of service as well as the findings from the application of the Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis (FTA) methods in evaluating operational risks in the Customer Identification File (CIF) process.

The presentation begins with a summary of the survey participants' profiles to provide context and data validity, followed by an explanation of the FMEA and FTA steps used to identify failure modes, calculate risk priorities, and map the main causal pathways

that could potentially disrupt the smooth management of the CIF. With this approach, we can gain a more comprehensive understanding of how human factors and systems interact to create risks, as well as the fundamentals for designing appropriate mitigation strategies.

Based on the results of the questionnaire distributed to 26 respondents, 65% are female and 35% are male. In terms of education, the majority, 62%, hold a Bachelor's degree (Stratum 1), 23% have a Master's degree, and 15% have a Diploma 3. The respondents' ages range from 26 to 55 years, with an average of around 41.6 years—half of them are between 37 and 46 years old—indicating that the CIF team is dominated by experienced workers. Based on the length of service at Bank Sumut, it varies quite a bit, ranging from newly joined to 32 years, with an average tenure of around 17.8 years and a median of 19 years. This indicates that most staff have served for more than a decade, so the combination of long experience and some relatively new employees provides a picture of the dynamics of competence and learning in CIF management.

Next, in this study, measurements of the questionnaire instrument were also conducted through validity and reliability tests. This is done to ensure that the data obtained truly reflects the actual conditions (valid) and is consistent across items (reliable). Validity testing is conducted by observing the item-total correlation, and reliability testing is conducted by observing the Cronbach's Alpha value. The majority of items have a correlation above 0.30, indicating that most of the questionnaire statements are valid for measuring the CIF operational variable. Additionally, the overall Cronbach's Alpha value of 0.830 indicates that the questionnaire instrument is classified as high (good). This means that respondents' answers between items tend to be consistent and homogeneous.

Based on the average responses from the respondents, there are several important findings that indicate potential sources of problems in the operational Customer Identification File (CIF) at PT Bank Sumut. The following is an estimate of the data processing results.

Table 5. Failure Mode and Effect Analysis (FMEA

No	Process	Failure Mode	Consequence	The main cause	S (1–5)	O (1–5)	D (1–5)	RPN (S×O×D)
1	Filling in CIF Data on CBS	Field/data ambigu (mis-entry)	Customer data is invalid, service is delayed/invalid, potential fraud/KYC failed.	Lack of understanding of SOP (average survey ~2.9)	4	3	4	48
2	Filling in CIF Data on CBS	Field that is not needed is entered	Database full of junk records, report inconsistencies, potential audit miscompliance	SOP for data updates is unclear (SOP survey median 4.3)	3	2	4	24
3	Document Verification	Documents (ID card/tax ID) are incomplete/blurred.	Account opening delayed, customers run to another bank, loss of income	The manual inspection system is only once, the SOP lacks detail.	4	3	4	48
4	Document Verification	Missing scan ID Card/tax ID	Customers cannot undergo complete KYC, potential regulatory fines.	Staff are in a hurry, no alert (D=5)	5	2	5	50
5	Synchronization CBS-ARS	Data mismatch (inkonsistensi)	Consolidated report incorrect, failed audit, OJK/BI sanctions – damaged reputation	Batch synchronization only once a day (O=3)	4	3	4	48
6	Synchronization CBS-ARS	ARS down / ARS module difficult to access	Can't open new accounts at the branch, long queue, frustrated customers	Error logs occur frequently (ARS survey 3.8)	3	2	3	18
7	Data Update / CIF Update	Daily data is not updated.	The information for tomorrow inaccurate incorrect report, wrong decision (credit/limit))	Backup job often times out (D=5)	4	2	5	40
8	Data Update / CIF Update	Old field still appears (SOP not followed)	Data lost due to old field deletion? customers protest, potential legal action	Staff have not yet been accustomed to the new SOP (objective survey ~4.3).	4	3	4	48

Source: data processed

First, the aspect of form completeness inspection received an average score of 4.62, indicating that most staff consistently check customer data before proceeding with the process. However, there is still a gap between the awareness of the importance of data verification and the implementation of thorough check-and-balance procedures, resulting in a relatively high chance of visible input negligence.

Second, the frequency of data input errors has an average value of around 4.42, which indicates that although employees feel that the mistakes they make are minor, in reality, at the branch level, these errors occur repeatedly. This implies that input errors are not considered significant by the operational team, leading them to be overlooked, even though the accumulation of small errors can result in database inconsistencies and potential disruptions in subsequent processes.

Third, the existence of Standard Operating Procedures (SOP) related to the opening and updating of customer data is recorded with an average score of 4.35. This means that, formally, the procedures and internal policies are available, but in reality, their implementation in the field is not always effective. Many staff members have difficulty understanding or accessing the SOP, so in daily practice, deviations are still found when filling out or updating CIF data.

Fourth, the understanding of each field or data in the Core Banking System (CBS) received an average score of 2.92. This figure falls within the "Neutral–Agree" range, indicating that there is a group of staff who are still unsure or lack confidence in how to fill out several important fields in the CBS. This uncertainty has the potential to cause the data entered to be inconsistent or not in the specified format.

Fifth, regarding the ease of use of the ARS (Analyzed Report System) module, respondents gave an average score of 3.81. This indicates that most staff find the CIF module in the ARS relatively easy to understand and use, although there is still a small portion who are not entirely comfortable or remain "Neutral" towards the work procedures within the system.

Sixth, data synchronization between CBS and ARS is also a concern. The statement "There is no data difference between the CBS application and ARS" received an average score of 3.27, while "There is no data difference between CBS and the CBS results report" received 3.88. This means that although most staff members stated that the data is quite consistent, the score not reaching the "Strongly Agree" level indicates that there are still occasional data inconsistencies in the system.

Lastly, external factors such as natural disasters or connectivity issues tend to occur infrequently, with an average score of 2.31 on the question about the frequency of natural disasters triggering the opening of mass accounts. Meanwhile, the hardware (PC) used received a score of 4.19, so it can be concluded that most of the hardware is currently adequate and not a major obstacle in CIF operations. All these findings indicate that although the infrastructure and formal SOPs are available, the biggest challenge still lies in the staff's understanding and diligence in the daily implementation of procedures.

Based on the explanation, the most critical modes in the CIF process obtained through the FMEA method are the failure to scan ID cards/NPWP (RPN=50), ambiguous data entry (RPN=48), inconsistency between CBS and ARS (RPN=48), and incomplete CIF updates (RPN 40–48). The failure to scan documents occupies the highest severity score (S=5) because it can result in regulatory fines and KYC failures, while ambiguous data and CBS–ARS mismatches (S=4) have the potential to disrupt services, damage reputation, and violate compliance. From the frequency perspective, ambiguous data errors and mismatches occur quite often (O=3), while ARS downtime is relatively rare (O=2). Most failures are only detected during monthly audits or problematic reports, resulting in a detection value at a difficult to nearly impossible level (D=4–5). Thus, the focus of improvement should be directed towards the implementation of early detection and prevention of ambiguous data input to reduce risks and strengthen the quality of the CIF process

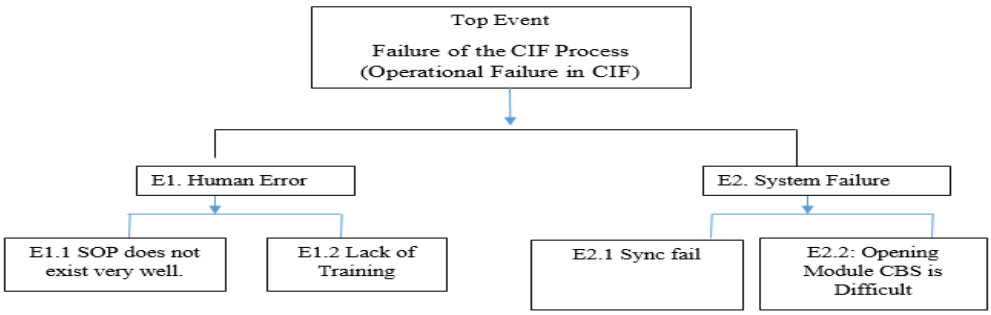


Figure 4. FTA Diagram

Figure 4, explain Fault Tree Analysis (FTA), the human error category (E1) is divided into two important sub-events. First, E1.1 (“SOP Not Available/Not Understood”) shows that although the formal SOP document is actually available—reflected in the

survey score of around 4.3—its implementation has not been optimal because the average staff has not fully understood how to fill in each field in the CBS, as indicated by the understanding score of only around 2.9. Second, E1.2 ("Lack of Staff Training") reveals the fact that many employees consider data input errors to be minor, indicating a lack of ongoing training; without routine training at least every six months, such errors will continue to occur. Meanwhile, under the system failure category (E2), there are two main sub-events. E2.1 ("Data Sync Failed") stems from inconsistencies between CBS and ARS—although the average respondents stated there was no data difference (score ~3.27), the fact that synchronization is only done once a day (Occurrence = 3) triggers a potential mismatch (Severity = 4, Detection = 4). E2.2 ("ARS/CBS Module Difficult") indicates that although most staff consider the CIF module in ARS relatively easy to use (score ~3.81), not everyone feels "Strongly Agree," resulting in some users experiencing lag or inconvenience, especially when the system is burdened with many requests (Severity = 3, Occurrence = 2, Detection = 3). Finally, if either E1.1 or E1.2 (human error) occurs—whether due to staff not understanding the SOP or being undertrained—then the entire CIF process is guaranteed to fail, as well as if the synchronization between CBS and ARS encounters issues, resulting in inconsistent data.

Based on the analysis a number of strategic recommendations have been formulated to mitigate the risk of errors in the customer data input (CIF) process. Reduce human error (E1.1 and E1.2) in the CIF process, institutions should simplify and clarify SOPs through visual aids, short video tutorials, and one-page quick-reference guides at workstations. These tools help staff understand how to correctly complete key data fields in the CBS system. In addition, structured training is essential. New staff should attend onboarding sessions focusing on KYC and system simulations, while all employees should receive refresher training every six months. Annual internal certification can ensure continued competence. A data quality culture must also be enforced through clear policies, including re-upload requirements for unclear documents and performance-based rewards or sanctions depending on error rates. The results of this study are in line with what has been done by (Fahmy 2020; Knežević 2013)

System improvements (E2.1 and E2.2) are also needed. Replacing batch synchronization with real-time API-based data syncing between CBS and ARS can prevent data mismatches. If errors occur, pop-up alerts should notify IT and branch staff immediately. Enhancing the user interface (UI) by adding features like auto-complete and built-in validation (e.g., ID number = 16 digits) will reduce input mistakes. An automatic error log system can help IT teams track recurring system issues. The CBS system should have validation checkpoints that prevent the storage of incomplete forms in order to enhance early detection (lower detection score). Important fields like ID number or ID tax can be verified with the use of OCR. Errors may be detected early with prompt feedback and a daily sample audit of new CIF entries per branch. To guarantee ongoing improvements in data quality and compliance, all concerns should be recorded in CAPA reports and monitored by the risk management team. These steps will not only reduce the identified operational risks but also strengthen regulatory compliance and maintain the quality of customer data, thereby supporting the smoothness and sustainability of banking services at PT Bank Sumut

5. Conclusion

Based on the results of the FMEA and FTA, it was found that human error is the main contributor to failures in the CIF process at PT Bank Sumut. The two highest failure modes—ambiguous field data (RPN = 48) and missing ID card/ ID tax scans (RPN = 50)—indicate that staff ignorance of SOPs and lack of training are the main factors increasing the risk. The batch-based synchronization system CBS–ARS also shows a high RPN value (48), although technological improvements are relatively easier to implement. Additionally, the detection value, which remains at a difficult to nearly impossible level (D = 4–5), confirms that many errors are only identified through monthly audits or complaint reports, resulting in failures often being addressed too late.

The implications of these findings are multidimensional. First, operationally, Bank Sumut needs to strengthen the understanding and implementation of SOPs through visual job-aids, video tutorials, and structured periodic training, so that the rate of data input errors can be minimized. Second, technological improvements such as real-time sync and automatic validation must be implemented to reduce mismatches between CBS and ARS, ensuring more reliable consolidation reports and regulatory compliance. Third, detection weaknesses necessitate the implementation of daily mini-audit mechanisms and early warning systems, so that the potential losses due to regulatory fines or tarnished reputation can be minimized more quickly. Strategically, this research emphasizes the need for the integration of people, process, and technology approaches in CIF operational risk management. In the long term, Bank Sumut is advised to implement a continuous improvement framework that includes revising SOPs whenever regulations change, periodically evaluating FMEA and FTA methods, and consistently measuring KPIs to monitor the effectiveness of mitigation efforts. These findings can also serve as a reference for other banking institutions facing similar challenges, while opening up opportunities for further research on the impact of technological interventions and continuous training on the quality of customer data and regulatory compliance

References

[1] Andrew Cornford. (2005). *Basel II: The Revised Framework of June 2004*.
[2] Andrianto, Fatihudin, D; Frimansyah., M. A. (2019). *Manajemen Bank*.

[3] Berger, Allen N., Filippo Curti, Atanas Mihov, and John Sedunov. (2018). "Operational Risk Is More Systemic than You Think :Evidence from U.S. Bank Holding Companies." 1(704).

[4] BSTDB. (2014). "Operational Risk Management Policy." *Black Sea Trade & Development Bank* 1–6.

[5] Cahyabuana, Brigitta Devianti. (2018). "Konsistensi Penggunaan Metode FMEA Terhadap Penilaian Risiko Teknologi Informasi (Studi Kasus : Bank XYZ)." *Jurnal Sistem Informasi* 1(2):5–11.

[6] Cardoso, António, and Marta Cardoso. (2024). "Bank Reputation and Trust: Impact on Client Satisfaction and Loyalty for Portuguese Clients." *Journal of Risk and Financial Management* 17(7).

[7] Coleman, Rodney. (2011). "Operational Risk." in *Wiley Encyclopedia of Operations Research and Management Science*.

[8] DeGroff, Jonathan, and Gene Jean Win Hou. (2025). "Fault Tree Analysis for Robust Design." *Designs* 9(1).

[9] Fahmy, Edian. (2020). "Analisa Pengukuran Beban Modal Risiko Operasional Metode Basic Indicator Approach (Bia) Dan Advance Measurement Approach (Ama) Di Bank Efg." *E-Mabis: Jurnal Ekonomi Manajemen Dan Bisnis* 21(1):14–20.

[10] Hull, John C. (2018). *Risk Management and Financial Institution, Fifth Edition*. Fifth. Canada: Wiley.

[11] Ierace, Stefano. (2010). "The Basics of FMEA, by Robin E. McDermott, Raymond J. Mikulak and Michael R. Beauregard." *Production Planning & Control* 21(1):99–99.

[12] Knežević, Marija. (2013). "Operational Risk–Challenges for Banking Industry." *Economic Analysis* 46(1–2):40–52.

[13] McDermott, Mikulak, Bearaugard.(2008). *The Basic of FMEA*. New York: Productivity Press.

[14] Meshcheriakov, Andrii, Anatoliy Maslov, Grygorii Saienko, Oksana Antoniuk, and Tetiana Sunduk. 2024. "Assessment of Factors Influencing the Stability of the Banking System: Experience of the European Union Countries." in *Salud, Ciencia y Tecnologia - Serie de Conferencias*. Vol. 3.

[15] Mulyati, Etty. (2018). "Penerapan Manajemen Risiko Sebagai Prinsip Kehati-Hatian Dalam Pemberian Kredit Perbankan." *SUPREMASI Jurnal Hukum* 1(1):34–48.

[16] Nurapiah, Dewi. (2019). "Manajemen Risiko Operasional Pada Perbankan Syariah Di Indonesia." *EKSISBANK: Ekonomi Syariah Dan Bisnis Perbankan* 3(1):66–73.

[17] Okeke, M. .., C. .. Aganoke, and AN Onuorah. (2018). "Operational Risk Management and Organizational Performance of Banks in, Edo State." *International Journal of Academic Research in Economics and Management Sciences* 7(4):103–20.

[18] Pangestuti, Dewi Cahyani, Heni Nastiti, and Renny Husniaty. (2021). "Failure Mode and Effect Analysis (FMEA) for Mitigation of Operational Risk." *Inovasi* 17(3):593–602.

[19] Pramudita, Dominicus Ervan Ricko. (2024). "Perlindungan Hukum Terhadap Data SLIK Debitur Pada Kasus Kesalahan Perusahan Fintech Dalam Memasukkan Data SLIK." *Iuris Studia Jurnal Kajian Hukum* 5(September):484–91.

[20] Ristanović, Vladimir, Dinko Primorac, and Goran Kozina. (2021). "Operational Risk Management Using Multi-Criteria Assessment (Ahp Model)." *Tehnicki Vjesnik* 28(2):678–83.

[21] Rosih, Akhmad Raunaq, Mochamad Choiri, and Rahmi Yuniarti. (2015). "Analisis Risiko Operasional Pada Departemen Logistik Dengan Menggunakan Metode FMEA." *Jurnal Rekayasa Dan Manajemen Sistem Industri* 3(3):580–91.

[22] Sari, Irna Meutia, Saparuddin Siregar, and Isnaini Harahap. (2020). "Manajemen Risiko Kredit Bagi Bank Umum." *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS) 2020* 1(1):553–57.

[23] Sutrisno, Sutrisno, Ludia Panggalo, Muhammad Asir, Muhammad Yusuf, and Pandu Adi Cakranegara. (2023). "Literature Review: Mitigasi Resiko Dan Prosedur Penyelamatan Pada Sistem Perkreditan Rakyat." *Journal of Economic, Bussines and Accounting (COSTING)* 6(2):1154–67.

[24] Testa, Mario, Antonio D'Amato, Gurmeet Singh, and Giuseppe Festa. (2024). "Innovative Profiles of TQM in Banking Management. The Relationship between Employee Training and Risk Mitigation." *TQM Journal* 36(3):940–57.

[25] Vasiliev, I. I., P. A. Smelov, N. V. Klimovskih, M. G. Shevashkevich, and E. N. Donskaya. (2018). "Operational Risk Management in a Commercial Bank." *International Journal of Engineering and Technology(UAE)* 7(4.36 Special Issue 36):524–29.