

**AN ANALYSIS OF THE ANTI-FRAUD STRATEGIES
IMPLEMENTATION IN MINIMIZING OCCUPATIONAL FRAUD
AT PT BPR BANK SLEMAN**

AN UNDERGRADUATE THESIS

Presented as a Partial Fulfillment of the Requirements
to Obtain the Bachelor Degree in the Accounting Department



By:

CHANTIKA RAHMA AGUSTINA

Student Number: 22312185

**INTERNATIONAL UNDERGRADUATE PROGRAM IN ACCOUNTING
FACULTY OF BUSINESS AND ECONOMICS
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2026**

**AN ANALYSIS OF THE ANTI-FRAUD STRATEGIES
IMPLEMENTATION IN MINIMIZING OCCUPATIONAL FRAUD
AT PT BPR BANK SLEMAN**

AN UNDERGRADUATE THESIS

Presented as Partial Fulfilment of the Requirements to Obtain a Bachelor Degree
in Accounting Department

By:
CHANTIKA RAHMA AGUSTINA
Student Number: 22312185

Aug 21/04/2026


**INTERNATIONAL UNDERGRADUATE PROGRAM IN ACCOUNTING
FACULTY OF BUSINESS AND ECONOMICS
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2026**

DECLARATION OF AUTHENTICITY

Herein I declare the originality of the thesis; I have not presented anyone else's work to obtain my university degree, nor have I presented anyone else's words, ideas or expressions without acknowledgement. All quotations are cited and listed in the bibliography of the thesis.

If in the future this statement is proven to be false, I am willing to accept any sanction complying with the determined regulation or its consequences.

Yogyakarta, April 22, 2026



A handwritten signature in black ink, appearing to read "Chantika Rahma Agustina".

Chantika Rahma Agustina

APPROVAL SHEET
AN ANALYSIS OF THE ANTI-FRAUD STRATEGIES
IMPLEMENTATION IN MINIMIZING OCCUPATIONAL FRAUD
AT PT BPR BANK SLEMAN

Written by:

CHANTIKA RAHMA AGUSTINA

Student Number: 22312185

Approved by

Content Advisor,

A handwritten signature in black ink, appearing to be 'Hendi Yogi Prabowo', with a stylized, somewhat abstract shape to the left of the main text.

Hendi Yogi Prabowo, S.E., M.For.Accy., Ph.D., CFrA, CAMS. April 21, 2026

Language Advisor,

A handwritten signature in black ink, appearing to be 'Alfi Zakiya', with a stylized, somewhat abstract shape to the left of the main text.

Alfi Zakiya, S.Kom., S.Pd.

May 11, 2026

YUDICIUM FINAL PROJECT EXAMINATION
A FINAL PROJECT ENTITLED
AN ANALYSIS OF THE ANTI-FRAUD STRATEGIES IMPLEMENTATION IN
MINIMIZING OCCUPATIONAL FRAUD AT PT BPR BANK SLEMAN

Written By : CHANTIKA RAHMA AGUSTINA

Students ID Number : 22312185

Defended before the Board of Examiners and Declared Acceptable

on day, date: Monday, May 18, 2026

Examiner/Content Advisor: Hendi Yogi Prabowo, S.E., M.For.Accy., Cfra., Ph.D.

Examiner : Suwaldiman, S.E., M.Accy., Ak., CMA.

Acknowledged by

Dean of the Faculty of Business and Economics

Universitas Islam Indonesia



Prof. Johan Arifin, S.E., M.Si., Ph.D., CfrA., CertIPSAS.

MOTTO

لَا يُكَلِّفُ اللَّهُ نَفْسًا إِلَّا وُسْعَهَا

Allah does not burden a soul more than it can bear (2:286)

I hope you recognize not only the result, but also the effort you've put into it.

You may be late, but hard work never betrays. So instead of believing you might never do it right, just do it, and keep in mind that you can do it.

Choi Yeonjun of TXT

“Memento mori, memento vivere”

PREFACE

Assalamu'alaikum Wr.Wb. Praise be to the presence of Allah SWT, for all His grace and guidance that has been bestowed on the researcher. With gratitude, the researcher invokes blessings upon Prophet Muhammad SAW for leading human life to a better path. Thus, the researcher can complete the final research assignment entitled "An Analysis of The Anti-Fraud Strategies Implementation in Minimizing Occupational Fraud at PT BPR Bank Sleman" which has been prepared as the partial requirement to obtain bachelor degree in the International Undergraduate Program in Accounting, Faculty of Business and Economics, Universitas Islam Indonesia. The completion of this research was made possible through the support of the following, to whom the researcher extends her sincere gratitude:

1. Allah SWT, for His blessings in life, strength, and longevity to finalize this research.
2. Rasulullah Muhammad SAW, as the best role model for Muslims.
3. Prof. Johan Arifin, S.E. M.Si. Ph.D., as the Dean of the Faculty of Business and Economics Universitas Islam Indonesia.
4. Prof. Rifqi Muhammad, S.E., S.H., M.Sc., Ph.D., as the Head of the Undergraduate Program in Accounting, and Ms. Yunice Karina Tumewang, S.E., M.Sc., SAS., Ph.D., as the Secretary of the International Undergraduate Accounting Study Program.
5. Mr. Hendi Yogi Prabowo, SE., M.For.Accy., Ph.D., CFrA., CAMS., as content advisor, and Ms. Alfi Zakiya, S.Kom., S.Pd., as language advisor, whose expertise and unwavering mentorship provided essential guidance throughout the completion of this research.
6. PT BPR Bank Sleman, for granting permission, their cooperation, and support, allowing me to conduct my research and complete this thesis.
7. Mrs. Maulidyati Aisyah, S.E., M.Com(Adv.), for giving me the opportunity to gain experience as a teaching assistant, and to all the lecturers in IUP Accounting for their invaluable knowledge and guidance shared during the researcher's academic journey.

8. To all IUP staff, for your constant assistance and all the pertinent information provided throughout this academic endeavor.
9. *Mama*, the strongest person the researcher has ever met. I wish that you could experience a life filled with greater personal joy and fulfillment, regardless of our maternal bond. Thank you for going above and beyond for our family.
10. *Papa*, thank you for stepping in support and unwavering faith in me between your absence. I just wish you were a better man.
11. The twin of family, Adzka & Azky, whose shoulders are full of loads but still showing up — thank you. I wish you happiness, always.
12. Dear little sister, Ayla. Thank you for being a friend in home, I hope life could be a little kinder to you.
13. *Fourtyone*, the researcher's timeless best friends. Kaysa, Asha, Salwa, Caca, Dinda, Ica, Aghnia, and Adillah whose presence is more than enough. I am truly obliged that our paths crossed and will continue to cross together.
14. Salima, Nurul, and Bitu, who have been by my side through the highs, the lows, and everything in between of this college journey. Thank you for being the kind of friends I did not know I needed, throughout the double lessons of college.
15. *Warjo*, especially *ciwciw*. Thank you for the happiness you brought in me. I will always cherish the memories we share.
16. Husna, Wijdan, Ulil, and all my classmates in IUP Accounting batch 2022, thank you for your spirit throughout my undergraduate journey. You've been wonderful classmates, and I truly appreciate the insightful discussions and enjoyable study sessions we had.
17. *Kak Nanda*, *Kak Hana*, *Kak Aul*, *Kak Shafa*, *Mas Iqbal*, and all fellows *Keluarga Pak Rokhedi*, specifically Public Relations 2023/2024. Thank you for being the beginning of my journey—where I grew from knowing nothing into someone who learned, adapted, and developed along the way. More than just a unit, this space has become a place where I feel I belong.

18. Adam, Alvaro, Abil, *Kak* Melly, and all members of *Keluarga Satu Lift*, especially Public Relations 2024/2025, whose laughter is bigger than the problems we faced. Thank you for remaining a place I could always return to, even when I was not around as much as I wished. I might not be at my best this time around, but something about you felt like home.
19. *Kak* Aini, Althaf, Echa, Lia, and all staff of Marketing and Communications FBE UII 2025/2026, particularly Public Relations team and *Koor* Marcomm. Thank you for being part of my journey during the completion of this thesis. Through all ups and downs, this period has become a meaningful closing chapter that reflects the growth, resilience, and experiences I have carried.
20. *Kak* Nida, Yurna, Ida, Azis, Ardi, PKM KI Sleep, IPF 2024, PKM Corner 2024, EO of Feskon 2022, and all people whose path crossed mine. You have helped broaden my perspective in life through unexpected ways, and for that, I'm sincerely pleased.
21. Tomorrow X Together, for the music that keeps me alive. Choi Yeonjun, Choi Beomgyu, Choi Soobin, Kang Taehyun, and Huenig Kai for saving my life, existing as the moodbooster to fully live my life.

Lastly, to myself—the researcher. Thank you for believing in yourself and being a person who felt enough to be on your own. Thank you for staying strong through all the conditions you said you weren't survived for. Thank you for always bouncing back each time it's hard. Thank you for bringing out the best of you in every moment.

LIST OF CONTENTS

TITLE PAGE	i
DECLARATION OF AUTHENTICITY	ii
APPROVAL SHEET	iii
YUDICIUM FINAL PROJECT EXAMINATION	iv
MOTTO	v
PREFACE	vi
LIST OF CONTENTS	ix
LIST OF TABLE	xii
LIST OF FIGURES	xiii
LIST OF APPENDICES	xv
ABSTRACT	xvi
CHAPTER I INTRODUCTION	1
1.1 Study Background	1
1.2 Research Problems	5
1.3 Research Objectives	6
1.4 Research Focus	7
1.5 Research Contributions	8
1.6 Systematics of Writing	9
CHAPTER II THEORETICAL REVIEW	11
2.1 Literature Review	11
2.1.1 Local Government-Owned Rural Bank.....	11
2.1.2 Fraud.....	14
2.1.3 Anti-Fraud Strategy	23
2.2 Prior Research	29
CHAPTER III RESEARCH METHODS	35
3.1 Type of Research.....	35
3.2 Research Object.....	36
3.3 Research Instrument	37
3.4 Research Systematics	37

3.5	Research Data Sources	39
3.5.1	Documents	39
3.5.2	Interviews	40
3.6	Data Collection Method	42
3.7	Data Analysis Method	43
3.7.1	Coding	43
3.7.2	Analytical Map	45
3.7.3	Matrix Coding Query	46
3.7.4	Framework Matrices.....	46
3.7.5	Conclusions	47
3.8	Data Validity Test.....	47
CHAPTER IV DATA PRESENTATION AND DISCUSSION		51
4.1	Profile of PT BPR Bank Sleman	51
4.1.1	History of PT BPR Bank Sleman	51
4.1.2	Organizational Structure of PT BPR Bank Sleman.....	55
4.1.3	Financial Profile of PT BPR.....	56
4.1.4	Products and Services of PT BPR Bank Sleman.....	61
4.2	Types of Occupational Fraud Potential at PT BPR Bank Sleman.....	62
4.2.1	Asset Misappropriation	69
4.2.2	Corruption.....	71
4.2.3	Financial Statement Fraud	73
4.2.4	Deception.....	74
4.2.5	Leakage of Confidential Information	75
4.3	Anti-Fraud Strategy Implementation.....	77
4.3.1	Prevention.....	88
4.3.2	Detection.....	101
4.3.3	Investigation, Reporting, and Punishment.....	109
4.3.4	Monitoring, Evaluation, and Further Action	112
4.4	Challenges Faced by PT BPR Bank Sleman in Anti-Fraud Strategy Implementation.....	115
4.4.1	Deficiencies	117

4.4.2	Implementation Barriers	119
4.5	Recommended Improvements Can be Made by PT BPR Bank Sleman	121
4.6	Conclusion	125
CHAPTER V CONCLUSIONS AND SUGGESTIONS		128
5.1.	Conclusions	128
5.2	Limitations.....	130
5.3	Suggestions.....	131
BIBLIOGRAPHY.....		133
APPENDICES.....		138

LIST OF TABLE

Table 3.1 Interviewee	42
-----------------------------	----

LIST OF FIGURES

Figure 2.1 Fraud Tree	18
Figure 4.1 Organizational Structure of PT BPR Bank Sleman	55
Figure 4.2 Total Assets of PT BPR Bank Sleman Year 2020-2024.....	57
Figure 4.3 Net Profit of PT BPR Bank Sleman Year 2020-2024.....	58
Figure 4.4 Loans Outstanding of PT BPR Bank Sleman Year 2020-2024	59
Figure 4.4 Loans Outstanding of PT BPR Bank Sleman Year 2020-2024	59
Figure 4.5 Ratio Trends of PT BPR Bank Sleman Year 2020-2024.....	60
Figure 4.6 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman	64
Figure 4.7 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman Focused on Asset Misappropriation and Corruption.....	65
Figure 4.8 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman Focused on Financial Statement Fraud, Deception, and Leakage of Confidential Information	66
Figure 4.9 Matrix Coding of Potential Occupational Fraud at PT BPR Bank Sleman	67
Figure 4.9 Matrix Coding of Potential Occupational Fraud at PT BPR Bank Sleman	68
Figure 4.10 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	79
Figure 4.11 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Prevention	80
Figure 4.12 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Detection.....	81
Figure 4.13 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Investigation, Reporting, and Punishment and Monitoring, Evaluation, and Further Action	82
Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	83
Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	84
Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	85

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	86
Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	87
Figure 4.15 Analytical Map of Challenges Faced by PT BPR Bank Sleman in Implementing Anti-Fraud Strategies	116
Figure 4.16 Analytical Map of Recommended Improvements in Enhancing Anti-Fraud Strategy Implementation at PT BPR Bank Sleman.....	122

LIST OF APPENDICES

Appendix 1. Certificate of Research Completion.....	138
Appendix 2. Interview Transcript 1: Mr. Dwi Handoyo Miharjo	139
Appendix 3. Interview Transcript 2: Mr. Arif Setiawan	151
Appendix 4. Interview Transcript 3: Mrs. Dian Chandra Dewi	164
Appendix 5. Interview Transcript 4: Mrs. Rizky Chitra	174
Appendix 6. Interview Transcript 5: Mrs. Rizky Chitra	177
Appendix 7. Interview Transcript 6: Mr. Dwi Handoyo Miharjo	185
Appendix 8. Interview Transcript 7: Mr. Arif Setiawan	193
Appendix 9. Interview Transcript 8: Mrs. Rizky Chitra	197
Appendix 10. Interview Transcript 9: Mrs. Dian Chandra Dewi	200
Appendix 11. Framework Matrix of Potential Occupational Fraud at PT BPR Bank Sleman	203
Appendix 12. Framework Matrix of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	213
Appendix 13. Framework Matrix of Challenges Faced by PT BPR Bank Sleman in Implementing Anti-Fraud Strategies	258
Appendix 14. Framework Matrix of Recommended Improvements in Enhancing the Implementation of Anti-Fraud Strategy at PT BPR Bank Sleman	266

ABSTRACT

The growing sophistication of fraud in the banking sector, particularly in rural banks, has increased the potential risk of occupational fraud and highlighted the importance of anti-fraud strategy implementation as preventive measures and part of internal control. This research was conducted at PT BPR Bank Sleman to examine the potential forms of occupational fraud and the implementation of anti-fraud strategies in minimizing those risks. This research applied a qualitative approach, a case study method, and data collection techniques through interviews with selected informants, along with related documents analysis. The finding demonstrated that PT BPR Bank Sleman had identified several potential forms of occupational fraud and had made an effort to prevent and minimize the occurrence of those risks by implementing anti-fraud strategy in accordance with applicable Financial Services Authority Regulation (POJK). However, there were shortcomings and obstacles that still need to be improved to enhance the efficacy of its implementation and to strengthen anti-fraud awareness across employees and related external parties in creating a zero-fraud environment.

Keywords: *Anti-Fraud Strategy, Fraud Prevention, Fraud Detection, Anti-Fraud Team, Occupational Fraud, Potential Fraud, Rural Bank*

CHAPTER I

INTRODUCTION

1.1 Study Background

Digitalization has emerged as a pivotal catalyst for transformation in modern society, particularly in the banking industry. In Indonesia, it is marked by the adoption of innovations such as mobile banking, blockchain, and artificial intelligence (Kardiman et al., 2025) which improve efficiency, speed, and convenience in financial services (Bakri et al., n.d.). These advancements have reshaped the way banks operate, expanding financial inclusion and transforming how products and services are accessible to larger societal groups (Akanfe et al., 2025; Breuer & Knetsch, 2023). Furthermore, technological developments continue to redefine the banking industry by overcoming the limitations of conventional systems and encouraging greater innovation in financial management (Akanfe et al., 2025). At the same time, however, the increasing use of technology has also introduced new operational complexities and risks within the banking industry.

One of the major risks faced by the banking sector is fraud, a pervasive global issue across industries that hinders sustainable economic development and causes billions of dollars in losses every year (ACFE, 2024). In Indonesia, the banking sector has become one of the vulnerable targets for fraudulent activities. Some fraud cases in the banking industry include the improper use of giro instruments by irresponsible employees, transaction embezzlement, fictitious

loans, fictitious building, fictitious customer installments, among others (Yanti & Hidayah, 2023).

Occupational fraud is one of the most damaging types of fraud because it can result in significant losses for businesses and have detrimental institutional effects (Obloh, 2023). According to ACFE (2024), banking and financial services along with manufacturing, recorded the largest number of cases. In the banking and financial services alone, 305 cases were reported with a median loss of USD 120,000. ACFE (2024) further explained that the most common forms of occupational fraud are asset misappropriation and corruption, whereas financial statement fraud is less common but has the highest median loss. The consequences of occupational fraud were beyond financial losses; it extends to the damage of institutional reputation, employee morale, and relationships with stakeholders (Apsari & Chariri, 2025).

Given the significant losses and institutional consequences caused by occupational fraud, organizations need a comprehensive understanding of its causes and preventive strategies to protect their assets and maintain operational integrity (Wang et al., 2019, 2023). In response to the growing fraud challenges in the banking industry, anti-fraud strategy has become an increasingly important regulatory concern in Indonesia. Earlier, Bank Indonesia issued Circular Letter Number 13/28/DPNP on 9th December 2011 concerning the Implementation of Anti-Fraud Strategy for Commercial Banks (Bank Indonesia, 2011). Recently, the Financial Services Authority or OJK issued POJK Number 12 of 2024 concerning the Implementation of Anti-Fraud Strategy for Financial Services (OJK, 2024).

This regulation reflects the urgency of enhancing fraud prevention, detection, and response mechanisms across financial institutions. The implementation of an anti-fraud strategy aims to support the development of zero-fraud organizations (Suhartono, 2016). Nevertheless, fraudulent activities remain persistent in the banking industry and continue to evolve along with changes in the financial and technological environment (Butcovan, 2015). As banking operations become increasingly digitized, more diverse and technically complex fraud schemes have emerged, highlighting the need for institutions to strengthen governance structures (Vanini et al., 2023).

This urgency is even more pronounced in rural banks or *Bank Perekonomian Rakyat* (BPR). This condition is reflected in the growing number of BPR closures in recent years. OJK reported a decline in the number of BPRs from 1,402 in December 2023 to 1,392 in March 2024, with more than 160 institutions having disappeared since 2020 (OJK, 2025). Dian Ediana Rae, Chief Executive of Banking Supervision at OJK, stated that several closures resulted from management's inability to rehabilitate the bank as well as irresponsible practices that violated prudential principles, including fraud (Ramli, 2024). Similarly, the Chairman of LPS, Purbaya Yudhi Sadewa, underlined that fraud and poor governance, rather than economic shocks, were among the main causes of rural bank failures in 2024 (Ramli, 2024). These conditions indicate that rural banks require strong top-management support to mitigate fraud risks, as early prevention and detection may strengthen organizational awareness and resilience against misconduct (Rustiarini et al., 2016). Previous research had also proposed various

approaches to improve fraud prevention and detection, such as developing fraud indicators or red flags (Rustiarini et al., 2016), strengthening collaborative cooperation (Butcovan, 2015), establishing anti-fraud committees (Suhartono, 2016), and using technology-based solutions such as machine learning and data analytics to reinforce fraud detection in the banking sector (Kamdjou et al., 2024; Mabior & Wanyama, 2024; Prabha et al., 2024). Consequently, the issuance of POJK Number 12 of 2024 demonstrates that the anti-fraud strategy implementation has also grown in importance and necessity for BPRs.

Within this context, PT BPR Bank Sleman constitutes a very pertinent location for the present study. PT BPR Bank Sleman plays a strategic role in regional financial services as one of the biggest rural banks in Sleman Regency and a regionally owned company under the Government of Sleman Regency. Hence, it is expected to uphold strong governance, prudential principles, and effective risk management supported by qualified human resources. The institutional position is then reinforced by the Bank's accomplishments including, its designation as the Best Performance BPR 2025 by Infobank Media Group in the asset class above one trillion rupiah (Bank Sleman, 2025), as well as a number of awards pertaining to public information disclosure and accountability, such as the Highest Score Public Institution in the BUMD Category in the Special Region of Yogyakarta, recognition as an Informative Public Institution, and appreciation for outstanding PPID/PLID performance (Bank Sleman, 2025). These achievements indicate that PT BPR Bank Sleman is beyond a financially strong institution, but also one that demonstrates commitment to transparency and public accountability. For this

reason, PT BPR Bank Sleman provides a strategically significant setting for examining how anti-fraud strategies are implemented in minimizing occupational fraud, particularly within a regional public banking institution that is expected to preserve both performance and governance quality.

1.2 Research Problems

Based on the above description, the research problems are as follows:

1. What types of occupational fraud potential exist at PT BPR Bank Sleman that are addressed through the implementation of anti-fraud strategies?

This research problem aims to identify and analyze the various types of occupational fraud that may arise within PT BPR Bank Sleman. The researcher will explore fraud risks across different areas and examine how these risks are addressed through existing anti-fraud strategies implemented by PT BPR Bank Sleman.

2. How does PT BPR Bank Sleman implement effective anti-fraud strategies to minimize the occurrence of fraud in line with the evolving trends issues?

In this research problem, the researcher will examine whether the strategies applied are aligned with applicable regulations and standards, as well as how these strategies are implemented in practice. Furthermore, this research will assess the effectiveness of these strategies in minimizing fraud and analyze their adaptability to current fraud trends.

3. What challenges are faced by PT BPR Bank Sleman in implementing anti-fraud strategies to minimize the occurrence of fraud?

This research problem aims to analyze the challenges encountered by PT BPR Bank Sleman in implementing its anti-fraud strategies. The researcher will explore various obstacles and constraints faced during the implementation process, including operational and organizational factors. Moreover, this research will examine how these challenges affect the effectiveness of the anti-fraud strategy within the organization.

4. What improvements can be made by PT BPR Bank Sleman to enhance the effectiveness of anti-fraud strategy implementation?

This research problem seeks to explore potential improvements in enhancing the implementation of anti-fraud strategies at PT BPR Bank Sleman. The researcher will analyze the current practices and identify areas that can be strengthened, based on the Bank's perspective. The research will then propose practical recommendations to improve the effectiveness and sustainability of anti-fraud strategy implementation.

1.3 Research Objectives

Based on the research background and research problems explained above, the research objectives are as follows:

1. To identify the potential forms of occupational fraud at PT BPR Bank Sleman, which is the basis for addressing through the implementation of anti-fraud strategies.
2. To analyze the implementation of anti-fraud strategies at PT BPR Bank Sleman in minimizing the occurrence of occupational fraud in line with the growing fraud complexity.

3. To examine the challenges faced by PT BPR Bank Sleman in implementing anti-fraud strategies to minimize occupational fraud.
4. To provide recommendations to enhance the effectiveness of anti-fraud strategies implementation at PT BPR Bank Sleman.

1.4 Research Focus

To ensure that the research problems and objectives are addressed systematically, this research establishes the following research focus:

1. Research Site : Head Office PT BPR Bank Sleman, located at Jl. Magelang KM 10, Tridadi, Sleman, Yogyakarta, 55511.
2. Research Aspect : The anti-fraud strategy implementation as an effort to minimize occupational fraud at PT BPR Bank Sleman.
3. Research Period : December 2025 - February 2026
4. Research Object : Individuals and organizational units responsible for anti-fraud strategies at PT BPR Bank Sleman, including the Internal Audit Department, Legal Compliance & APU-PPT Department, Risk Management Department, and the Human Capital Department.

1.5 Research Contributions

This research is expected to provide benefits to related parties, including:

1. For the Researcher

This research is expected to deepen the researcher's understanding of the practical implementation of anti-fraud strategies within the rural banking sector, particularly in minimizing occupational fraud. Through a qualitative method, this research enhances the researcher's analytical skills in exploring fraud issues, interpreting organizational practices, and identifying implementation gaps between the policies and actual practices.

2. For PT BPR Bank Sleman

This research may serve as a valuable reference for PT BPR Bank Sleman in providing practical insights into the effectiveness of the current implementation of anti-fraud strategies. The findings are expected to assist management in identifying the current anti-fraud strategies implementation shortcomings. Additionally, the research offers constructive recommendations that can be utilized as a guide to improve the implementation of anti-fraud strategies.

3. For Other Parties

This research is projected to grow academic research in areas of accounting, auditing, and fraud risk management, particularly in the rural banking sector in Indonesia. The findings contribute as a reference for future research on occupational fraud and anti-fraud strategies implementation, especially using qualitative approaches. Likewise, this

research may provide comparative insights and best practices in implementing anti-fraud strategies.

1.6 Systematics of Writing

The writing systematics used in this research are as follows:

CHAPTER I: INTRODUCTION

This chapter contains the research background, problems, venue, objectives, contribution, and writing systematics.

CHAPTER II: THEORETICAL REVIEW

This chapter contains the theories used as a foundation for the research and can assist the researcher in addressing the research issues. This chapter also covers the conceptual basis for this study, prior research that is applicable to it, and helps researchers with fieldwork.

CHAPTER III: RESEARCH METHOD

This chapter describes the conducted research activities, including the type of research, research focus, research methodology, data sources and types, research objects, data collection techniques, data validity testing, and data analysis techniques.

CHAPTER IV: DATA PRESENTATION AND DISCUSSION

This chapter outlines the results of the analysis conducted based on the research. The analysis results are methodically

arranged in accordance with the problem formulation that was previously established.

CHAPTER V: CLOSING

This chapter contains the conclusions of the research conducted, limitations encountered during the research, and recommendations for further research.

CHAPTER II

THEORETICAL REVIEW

This chapter covers the theoretical foundation and literature review that support the conduct of this research and serve as the basis for the researcher's conceptual framework. To strengthen the development of the research framework, various theories and concepts are presented and described in depth. This is essential for a deeper understanding of the problems associated with this research, as well as for reviewing previous research relevant to the topic. This chapter discusses PT BPR Bank Sleman, anti-fraud strategy, and occupational fraud.

2.1 Literature Review

The literature review in this chapter provides a brief overview of the theories used by the researcher as a basis to conduct this research. The theories used include:

2.1.1 Local Government-Owned Rural Bank

According to Kemendagri RI (2024), in the Permendagri Regulation Number 21/2024 regarding the Local Government-Owned Rural Banks, a local government-owned rural bank (*Bank Perekonomian Rakyat Milik Pemerintah Daerah*) is a BPR whose capital is wholly or partly sourced from regional Government equity participation. This equity participation constitutes regional investment in the form of money and/or regional assets that may be recognized as capital or shares within the bank.

Local government-owned rural banks, as a local financial intermediary, go beyond business operations. Permendagri Regulation

Number 21/2024 outlines that these institutions are intended to strengthen regional economic development, expand financial access, support effective and efficient MSMEs financing, uphold good governance practices, and ensure sustainable profitability. To achieve these objectives, BPRs are authorized to conduct a wide range of activities as regulated under the Article 2 of this regulation, including:

1. Mobilizing public funds through savings, time deposits, and other equivalent deposit products;
2. Distributing funds in the form of credit or sharia-compliant financing;
3. Conducting fund transfers for the bank's own interest or on behalf of customers;
4. Placing funds in other banks, borrowing from other banks, or lending funds to other banks;
5. Conducting foreign exchange activities;
6. Making equity investments in supporting institutions of local government-owned BPRs within legal limits;
7. Establishing cooperation with financial service institutions and non-financial institutions in providing financial services to customers;
8. Carrying out receivables transfer activities;
9. Conducting other activities with OJK's approval.

In addition, activities regulated in article 4, including:

1. Mobilizing funds from regional governments, village governments, regional-owned enterprises, and regional public service agencies through savings, deposits, or equivalent instruments;
2. Optimizing banking services to support regional Government programs and activities according to prevailing laws;
3. Providing national and regional MSMEs credit schemes;
4. Supporting village governments by acting as the village treasurer and distributing village funds according to regulatory appointments by the regent.

Given the wide range of activities they engage in, BPRs unavoidably encounter various business risks. According to OJK (2015), business risk is the level of uncertainty surrounding expected outcomes that might cause the bank to suffer financial losses. The main risks faced by BPRs under OJK Regulation Number 13/POJK.03/2015 are as follows:

1. Liquidity Risk, the risk arising from the bank's inability to fulfill its maturing obligations due to insufficient cash flow or liquid assets;
2. Credit Risk, the risk emerges when borrowers or other counterparties fail to meet their financial commitments to the bank;
3. Operational Risk, the risk caused by inadequate or failed internal processes, human errors, system failures, or external events that disrupt the bank's operations;

4. Compliance Risk, the risk that occurs when the bank does not adhere to applicable laws and regulatory requirements;
5. Reputation Risk, the risk of declining stakeholder trust resulting from negative perceptions about the bank;
6. Strategic Risk, the risk arising from inappropriate or poorly executed strategic decisions made by the bank.

2.1.2 Fraud

2.1.2.1 Definition of Fraud

There may be no established definition of fraud. However, according to ISA 240, fraud refers to an intentional act carried out by one or more individuals within management, employees, or third parties, involving deceit to obtain an unlawful advantage. In practice, fraud inherently involves deliberate acts of concealment, misrepresentation, or manipulation intended to secure financial or personal gain at the expense of others (Gupta & Gupta, 2025, p. 2). Matthew et al. (2013) further emphasized that fraud involves intentional omission, distortion, or perversion of truth aimed at gaining unfair benefits, including causing another party to surrender something of value or a legal right, or inflicting harm in various forms. These definitions show that fraud is more than just a procedural violation; it is an intentional, ethically motivated act that is frequently committed by individuals who possess intelligence,

experience, and are aware of internal control but lack morality and integrity (Duffield & Grabosky, 2001, p. 2).

Fraud may occur in any organization, regardless of its size, industry, or geographical location (ACFE, 2024). According to Sudarmo et al. (2008), in practice, fraudulent activities may take place at all levels within an organization, ranging from top management to frontline employees, and even support staff. Fraud can be committed by anyone, including employees who appear to be honest.

Likewise, fraud committed by employees and management tends to flourish in a permissive organizational environment, where opportunities for fraud are implicitly encouraged. To prevent fraud, organizations must establish a firm and disciplined environment. Management is required to set clear policies and procedures that demonstrate a strong commitment to fairness, the avoidance of conflicts of interest, the encouragement of employee integrity, robust internal controls, and the imposition of severe penalties against fraud perpetrators (Sawyer et al., 2005).

2.1.2.2 Occupational Fraud

Occupational fraud refers to fraudulent acts committed by individuals within an organization who exploit their occupational positions for personal gain (Petersen et al., 2018). In this context, the Association of Certified Fraud Examiners, known as ACFE

(2024), defined occupational fraud as fraudulent acts committed by individuals against the organization that employs them.

This kind of fraudulent behavior is not limited to a specific organizational level. Shanikat et al. (2014) explained that occupational fraud may occur across hierarchical relationships, where fraud can be committed by employees against their superiors or, conversely, where fraud is perpetrated by superiors while employees become the victims. This indicates that occupational fraud is closely linked to the misuse of authority and trust embedded in organizational roles. Consequently, occupational fraud is often associated with white-collar crime, as it involves individuals in professional positions who abuse entrusted responsibilities for personal benefit (Cheliatsidou et al., 2023).

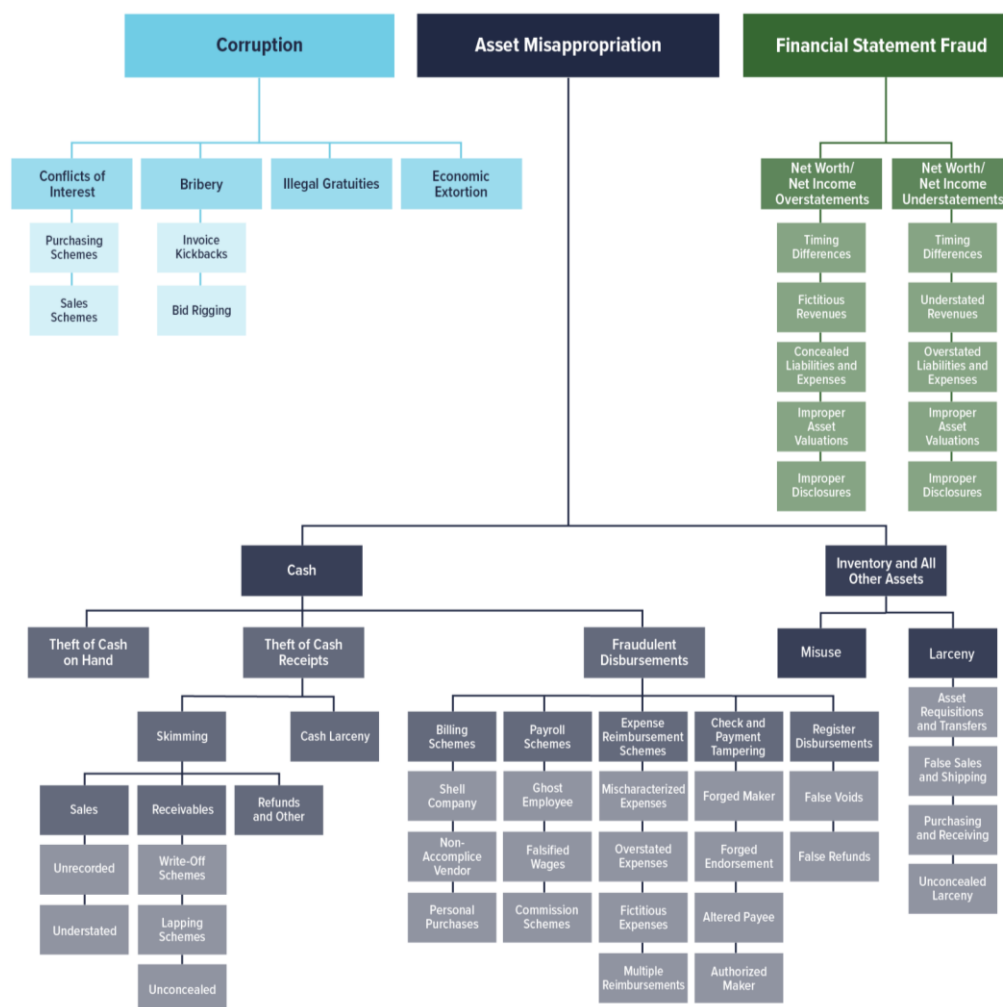
The significance of occupational fraud is further reflected in global empirical evidence. Based on data collected from Certified Fraud Examiners (CFEs) worldwide who participated in the Global Fraud Survey, ACFE (2024) reported a total of 1,921 occupational fraud cases across 138 countries, resulting in aggregate losses of approximately USD 3.1 billion. This evidence underlines that occupational fraud represents a substantial risk to organizations across various sectors.

Peltier-Rivest (2009) stated that occupational fraud is most likely to increase in organizations that do not have a specific

department dedicated to monitor employee behavior. Hence, effective supervision plays a crucial role in fraud prevention, as individuals who intend to commit fraud tend to actively seek and exploit weaknesses within existing standards. Similarly, Nawawi and Salin (2018) noted that deficiencies in organizational procedures can foster an environment that enables and encourages the occurrence of fraud.

2.1.2.3 Classification of Fraud

The Association of Certified Fraud Examiners (ACFE) schematically classifies fraud using the fraud tree framework.



Source: ACFE (2024)

Figure 2.1 Fraud Tree

The fraud tree framework, shown in Figure 2.1, illustrates the range of fraudulent activities that can arise within employment relationships across organizations. Based on this, occupational fraud is classified into three main categories, namely:

1. Asset Misappropriation

Asset misappropriation arises when employees exploit their access to organizational resources by unlawfully using

or taking assets for personal gain. Such fraud might involve cash and non-cash resources. Accordingly, asset misappropriation consists of:

- a. Cash misappropriation, it refers to fraudulent acts involving the diversion or theft of organizational cash.
- b. Non-cash misappropriation, it involves the unauthorized use or appropriation of non-cash assets such as facilities, equipment, or other tangible assets.

2. Financial Statement Fraud

Financial statement fraud refers to intentional misconduct committed by individuals in positions of authority within organizations, aimed at distorting the actual financial condition of the entity. This kind of fraud is carried out through deliberate manipulation of financial information in order to create misleading reports that provide unlawful advantages (Saputra, 2017).

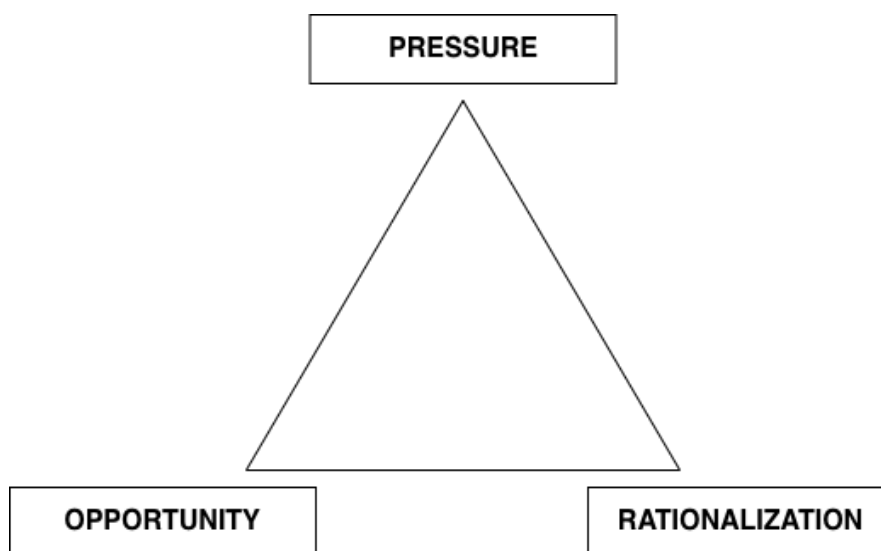
3. Corruption

Corruption represents a pervasive form of occupational fraud that frequently emerges in institutional environments with weak law enforcement and insufficient implementation of good governance practices, which in turn undermines organizational integrity. This fraud type is particularly difficult to uncover due to the involvement of multiple

parties who mutually benefit from the misconduct. Corrupt practices commonly include abuse of authority or conflicts of interest, illegal gratuities, and economic extortion (Kennedy & Siregar, 2017).

2.1.2.4 Fraud Triangle Theory

The fraud triangle theory developed by Cressey (1953) explained the underlying factors that drive individuals to commit fraud. Based on this theory, fraud occurs only when three essential elements are present, which are opportunity, pressure, and rationalization. If one of these elements is absent, fraud is unlikely to occur. This framework has been widely adopted in accounting and auditing literature, particularly in the bank sector's fraud risk.



Source: Cressey (1953)

Figure 2.2 Fraud Triangle Theory

The fraud triangle, shown in Figure 2.2, consists of opportunity, pressure, and rationalization, which collectively

contribute to the occurrence of fraud. The following discusses each factor:

1. Opportunity

Opportunity refers to situations that allow individuals to commit fraud. According to Buchholz (2012), based on Statement on Auditing Standards (SAS) No. 99, opportunity can be classified into:

- a. Nature of industry, it refers to industry characteristics or operational conditions that provide greater opportunities for fraudulent financial reporting, such as complex transactions or high levels of estimation;
- b. Ineffective monitoring, it includes weak oversight by the board of directors, unstable organizational structure, and ineffective internal control components.

Despite being able to be committed by anyone, management tends to have greater opportunities than employees due to broader access to assets, authority, and sensitive information (Putri, 2012). Fraud perpetrators tend to be highly adept at identifying weaknesses within organizational systems and exploiting them to their advantage. Typically, individuals commit fraud by abusing their position or authority, such as manipulating policies to facilitate fraud.

2. Pressure

Pressure refers to the motivation or incentive that drives an individual to commit fraud. Buchholz (2012), based on SAS No. 99, classified pressure into four main categories:

- a. Financial stability, it is the kind of pressure that arises when a company's financial condition is threatened by economic changes, declining performance, or unfavorable market conditions;
- b. External pressure, it is the kind of pressure that occurs when management relies heavily on external financing sources, such as debt or investor funding, to sustain business operations;
- c. Personal financial need, it refers to situations where executives or managers have a significant personal financial interest tied to the company's performance, such as share ownership;
- d. Financial targets, it refers to the performance benchmarks set by top management or the board of directors that must be achieved within a specific period of time.

3. Rationalization

Rationalization is the mental process by which individuals justify fraudulent behavior as acceptable. Fraud

perpetrators often convince themselves that their actions are justified, temporary, or harmless. Arens et al. (2015) found that individuals who commit fraud frequently seek moral justification by believing that their actions do not constitute a serious offense or that they are entitled to the benefits obtained. This rationalization reduces feelings of guilt and increases the likelihood of repeated fraudulent behavior.

2.1.3 Anti-Fraud Strategy

OJK (2024) in POJK No.12/2024 concerning the Implementation of Anti-Fraud Strategy for Financial Services Institutions, the anti-fraud strategy implementation is a mandatory element in fraud risk control required for all financial services institutions, including rural banks. The objective is to enhance the internal control as an effort to minimize and control fraud risk effectively. In accordance with this, the anti-fraud strategy implementation is carried out through a fraud control system backed by four interconnected pillars, which function collectively as an integrated framework for fraud prevention, detection, investigation, and monitoring activities in order to establish an anti-fraud culture across the company.

2.1.3.1 Prevention

The prevention pillar contains mechanisms designed to reduce the risk of fraud occurrence, including:

1. Anti-Fraud Awareness

This represents efforts to foster awareness regarding the importance of fraud prevention among all levels of the organization. Likewise, management should have significant influence on raising awareness and morale among all relevant parties through the policies they set and active supervision. Anti-fraud awareness may be implemented through the following strategies:

- a. Socialization of the formulation and implementation of anti-fraud statements, including a zero-tolerance policy for fraud;
- b. Anti-fraud culture programs for employees, conducted through continuous seminars, workshops, or training related to anti-fraud policies and procedures, fraud types, transparency in handling processes, and follow-up actions;
- c. Consumer fraud awareness and vigilance programs involve written explanations, banners, brochures, and other communication media to raise consumer awareness of possible fraud.

2. Fraud Risk Identification

This includes the process of identifying, analyzing, and evaluating fraud risk. It may be conducted periodically or at

any time when fraud indications arise for all activities, both internal and external information. Ultimately, it aims to identify inherent fraud risks that could result in losses for the organization. The result of this process must be documented, communicated to relevant parties, and updated periodically for activities deemed to have a high risk of fraud.

3. Know Your Employee

This serves as part of the human resource controls in the fraud prevention strategy. It is started through an effective recruitment procedure to perform a complete background check, continued by objective and transparent procedures for employee selection, placement, and promotion. This process is complemented by continuous monitoring of employees' integrity, behavior, and lifestyle, especially for positions exposed to a high risk of fraud.

2.1.3.2 Detection

The detection pillar aims to identify and detect fraud. The tools used in this pillar involve:

1. Whistleblowing System

This system is designed to enhance fraud detection by encouraging the disclosure and reporting of suspected fraud

by whistleblowers, both internal and external. This policy encompasses:

- a. Protection for whistleblowers;
- b. Regulations governing fraud reports;
- c. Fraud reporting systems and follow-up mechanisms.

All these policies should be applied consistently and transparently to build trust in the whistleblowing system's reliability and confidentiality.

2. Surprise Audit

This mechanism is performed to enhance employees' awareness and compliance, especially within business units and activities exposed to high fraud risk. This audit is conducted without prior notice to increase the effectiveness of detecting irregularities.

3. Surveillance System

This consists of discreet monitoring and examination activities conducted without the awareness of the examined parties to assess the effectiveness of anti-fraud policies. It may be carried out periodically or as needed.

2.1.3.3 Investigation, Reporting, and Punishment

This pillar encompasses the mechanisms related to handling detected fraud through investigation, reporting procedures, and imposition of punishment.

1. Investigation

Investigation is a critical component of the fraud control system, conducted to collect and analyze evidence related to detected fraud incidents. This process reflects that all fraud indications are handled in accordance with established standards and applicable regulations. Companies are expected to implement investigation standards, at a minimum, which involve:

- a. The designation of authorized investigators with due consideration to their independence and competence;
- b. Investigation procedures to follow up on detection results while maintaining the confidentiality of the information obtained.

2. Reporting

Companies are required to establish effective reporting procedures for investigation results, including internal reporting and reporting to OJK.

3. Imposition of Punishment

Companies are required to formulate internal punishment policies in response to the investigation's findings to provide a deterrent effect for fraud perpetrators, which are implemented fairly, transparently, and consistently. These policies shall at least include:

- a. Types of punishment based on the violations committed;
- b. Mechanisms for imposing punishment;
- c. Authorized parties are responsible for imposing punishment.

2.1.3.4 Monitoring, Evaluation, and Further Action

This pillar contains the strategies implied for monitoring, evaluating, and taking further action for fraud incidents, including:

1. Monitoring

One of the most important steps in implementing a fraud control system is keeping an eye on the follow-up actions of fraud incidents. Naturally, the company's internal regulations and relevant laws must serve as the base for this process.

2. Evaluation

The purpose of the evaluation is to identify weaknesses and the reasons behind fraud so that appropriate improvements can be decided. Inevitably, in order to facilitate the identification process, companies must keep fraud incident data (fraud profiling) prior to conducting the evaluation.

3. Further Action

Based on the evaluation results, companies need to implement the recommended improvements in order to strengthen the internal control system, solve weaknesses, and prevent the recurrence of fraud incidents.

2.2 Prior Research

This section covers the author's discussion regarding the prior research that are relevant to the current research. This research served as comparative references in assessing the effectiveness of anti-fraud strategies. By analyzing previous research, this research is positioned within the broader academic discourse on occupational fraud prevention and detection, particularly in rural banking.

Miharjo (2018), in "*Kajian Optimalisasi Peran Auditor Internal dalam Penerapan Sistem Anti Fraud (Studi Kasus Bank Sleman)*," analyzed how governance structures and internal control influence the effectiveness of occupational fraud prevention. The research found that the success of anti-fraud implementation is highly dependent on the clarity of role segregation, the independence of supervisory functions, and the consistency of internal audit practices. Weak separation among operational duties, supervisory oversight, and audit responsibilities is identified as a significant factor that increases fraud risk exposure, as overlapping functions create opportunities for misconduct. The research emphasizes the importance of applying the three lines of defense model, where management and compliance units, and internal audit functions operate

independently yet cohesively to ensure effective monitoring. Furthermore, as leadership commitment impacts organizational integrity and compliance culture, it has been discovered that robust board oversight and ethical leadership are essential for bolstering anti-fraud strategies. To maintain fraud prevention measures, the research also emphasizes the need for regular internal control effectiveness assessments, clear reporting procedures, and frequent fraud awareness training. Nevertheless, the results show that without ongoing supervision and managerial support, anti-fraud strategies could just become procedural. Thus, the research concludes that to minimize occupational fraud in rural banking institutions, effective anti-fraud implementation necessitates not only formal governance frameworks but also regular supervision, independent control functions, and the incorporation of fraud risk management into daily operational activities.

Hidajat (2020), in “Rural Banks Fraud: A Story from Indonesia,” investigated the root causes of fraud in Indonesian rural banks (BPR) and proposed strategies to mitigate such financial misconduct. The research identified four primary determinants of fraud, conceptualized through the fraud diamond framework (pressure, opportunity, rationalization, and capability). Among these elements, opportunity emerges as the most dominant factor, largely driven by limited human resources, dual roles of directors and shareholders, and weak supervisory mechanisms. Fraud perpetrators are driven not only by financial pressures, such as inadequate salaries, but also by non-financial factors like greed and discontent with the company. The paper suggests both internal and external anti-fraud strategies to solve these problems. Banks are urged to increase

organizational integrity, undertake proactive fraud audits, deploy red flag monitoring systems, institutionalize comprehensive anti-fraud strategies, and utilize big data analytics to manage risks. Externally, emphasis is placed on cooperation with regulators and the public, stronger law enforcement, and more transparent penalties. Overall, anti-fraud strategies are seen as essential tools for fostering an ethical culture, improving employee competence, and strengthening internal controls to prevent and detect fraud in rural banks.

Fajria (2023), in *“Penerapan Strategi Anti Kecurangan dalam Meminimalkan Occupational Fraud pada PT Bank X Cabang Kota Tarakan,”* focused on the practical execution of anti-fraud frameworks within a banking branch environment. The research assessed the institution’s preventive, investigative, and follow-up actions using a qualitative research approach that includes interviews and document analysis using NVivo 12 software. The findings revealed that PT Bank X has implemented a whistleblowing system as a key tool to promote open reporting of misconduct. To maintain neutrality and anonymity, an independent consultant oversees this reporting channel, called AYO LAPOR. Additionally, the bank continuously upholds integrity and moral behavior by implementing the principles of Good Corporate Governance. The research finds that the anti-fraud mechanisms generally comply with Bank Indonesia Circular Letter Number 13/28/DPNP. However, practical challenges remain evident, including limited employee awareness of anti-fraud strategies, reluctance to report colleagues due to fear of retaliation, and prolonged investigation processes that reduce efficiency.

Hana (2023), in “*Penerapan Strategi Anti Fraud dalam Meminimalkan Occupational Fraud pada PT BPR Danagung Bakti Yogyakarta*,” examined the implementation of anti-fraud strategies in rural banking operations. The research employed a qualitative approach through interviews and document analysis to evaluate how the anti-fraud framework operates in practice. The findings indicated that PT BPR Danagung Bakti Yogyakarta has adopted an anti-fraud strategy based on four main pillars in accordance with Bank Indonesia regulations, namely prevention, detection, investigation, and reporting with penalties, as well as monitoring and evaluation. This structured framework reflects the institution’s formal commitment to strengthen internal control and fraud risk management. However, the research also points out several implementation shortcomings. These include overlapping work duties, a lack of human resources, and supervisory tasks that have not yet been performed at their best. Evaluation activities are not always carried out regularly, which lowers the efficacy of early fraud detection systems. The research concluded that while PT BPR Danagung Bakti Yogyakarta’s anti-fraud strategy formally complies with relevant regulatory standards, its actual implementation still needs to be strengthened, especially in terms of human resource capacity, consistency of internal control application, and the effectiveness of monitoring and evaluation procedures. Hence, the research emphasized that regulatory compliance alone is insufficient unless each anti-fraud pillar is consistently and effectively integrated into daily operational activities.

Fajri and Prabowo (2024), in “*Fraud Threats: How Organization Improves The Anti-Fraud Team Quality?*” examined the role of human resources quality in

strengthening the implementation of anti-fraud strategies within banking institutions. According to the research, the competence, independence, and professional skepticism of anti-fraud teams have a major impact on the efficacy of occupational fraud mitigation. The research revealed that an organization's capacity to identify and address intricate fraud schemes is weakened by deficiencies in investigative abilities, analytical capacity, and cross-departmental collaboration. Specifically, the professional judgment needed to perform fraud tests is diminished by inadequate training and a lack of specific certification. The study highlights that to preserve neutrality when resolving fraud cases, anti-fraud teams need to maintain organizational independence in addition to have technical expertise. Moreover, structured training programs, competency-based hiring, continuous professional development, and periodic performance evaluations are identified as essential measures to enhance the quality of anti-fraud teams. The research concluded that strengthening the capability and integrity of anti-fraud personnel is a critical strategic component in ensuring that anti-fraud strategies function effectively in practice, thereby contributing directly to the minimization of occupational fraud risk.

The current research differed from prior research on both its research object and analytical focus. Previous research has generally examined fraud in rural banks and other banking institutions from a broader perspective, emphasizing general fraud risk factors, governance deficiencies, and regulatory compliance. In contrast, this research specifically concentrates on occupational fraud by analyzing the practical implementation of anti-fraud strategies at PT BPR Bank Sleman. This

focus is particularly significant given the increasing trend of internal fraud cases within rural banking institutions, where misconduct is often closely linked to employee behavior, weaknesses in internal controls, and governance structures. Even while some previous research was carried out in rural banks in Yogyakarta, they investigated different institutions and organizational contexts. Thus, by considering PT BPR Bank Sleman as an independent organization with unique governance traits, internal control systems, and implementation procedures, this research offered a unique institutional viewpoint. This research aimed to assess the degree to which anti-fraud strategies are successfully applied in reducing occupational fraud, taking into account that each Rural Bank (BPR) may interpret and operationalize anti-fraud policies differently, even though they comply with rules issued by the Financial Services Authority (OJK). The research adopted a qualitative case research approach, with data collected through direct interviews with relevant internal parties and analysis of supporting company documents, which are subsequently processed using NVivo 15 software to ensure systematic coding and rigorous interpretation. Furthermore, this research offered a comparative evaluation between the actual implementation of anti-fraud strategies at PT BPR Bank Sleman and the regulatory anti-fraud standards applicable to Rural Banks in Indonesia, thereby assessing whether formal compliance is accompanied by effective operational execution in reducing occupational fraud risk.

CHAPTER III

RESEARCH METHODS

This chapter provides the research methodology used to analyze the implementation of anti-fraud strategies in minimizing occupational fraud at PT BPR Bank Sleman. The discussion in this chapter serves as the framework for conducting the research and addressing the formulated research questions. It covers the type of research, research object, research instrument, research systematics, research data source, data collection method, data analysis method, and data validity test.

3.1 Type of Research

The approach employed in this research is a qualitative method with a case study technique. Qualitative research is inherently flexible and unstructured, prioritizing the role of research subjects and enabling a deep exploration of specific cases. Instead of using statistical methods, data analysis is done descriptively and interpretively (Hammersley, 2013). Within this approach, a qualitative case study enables the researcher to investigate a phenomenon in its actual context by utilizing various data sources, facilitating the object to be understood from numerous perspectives (Baxter & Jack, 2015). Accordingly, this research intends to provide an extensive and intricate representation of the phenomenon being studied, expressed through in-depth narrative explanations that produce rich and contextualized insights obtained straight from primary information sources (Fadli, 2021).

As explained, this research employed a qualitative approach through direct interaction with selected informants to gather data that accurately represents the organization's actual conditions. PT BPR Bank Sleman, as the object of this research, is examined and analyzed in relation to the implementation of the anti-fraud strategies in minimizing occupational fraud, especially in response to the changing patterns of fraud issues in rural banking institutions. To guarantee the reliability and consistency of the data collected, the researcher conducts interviews to gain in-depth data with relevant internal parties and supports the findings with related company documents. Furthermore, this research identified the types of potential occupational fraud handled by the current anti-fraud framework. The research also compared the bank's internal policies with regulatory standards issued by the Financial Services Authority (OJK). Additionally, the research assessed the challenges faced by PT BPR Bank Sleman in implementing its anti-fraud policies. Based on these results, the research offered suggestions for improving the efficiency of anti-fraud strategy implementation and bolstering the organization's ability to reduce the risk of occupational fraud.

3.2 Research Object

The object of this research was PT BPR Bank Sleman, particularly the individuals and organizational units responsible for the implementation of anti-fraud strategies within the institution. The details of the analysis were based on the findings of comprehensive interviews with selected informants. These informants were representatives from the Internal Audit Department, Legal Compliance and

APU-PPT Department, Risk Management Department, and Human Capital Department.

3.3 Research Instrument

The researcher was the main instrument in qualitative research, which means that the investigator was directly involved in data collection and interpretation. To gather the information and insights needed for the research, the researcher interviews data providers directly. Within this approach, the researcher was considered the most influential instrument in the research process, as the depth, accuracy, and interpretation of findings largely depend on the researcher's involvement and analytical capability (Fadli, 2021). In the meantime, the research object served as the knowledge base that advances new comprehension (Leavy, 2014). Furthermore, as the main instrument, the researcher must spend enough time in the organizational environment under study to collect comprehensive data and conduct extensive analysis (Hancock & Algozzine, 2006).

3.4 Research Systematics

The systematic procedure of qualitative research refers to the series of steps undertaken during the research process, from the study's inception to its end, which covers the planning, executing, data analysis, and drawing conclusions. The structure and sequence of these steps may vary across studies, depending on the specific research topic. The following outlines the research procedure applied in this research:

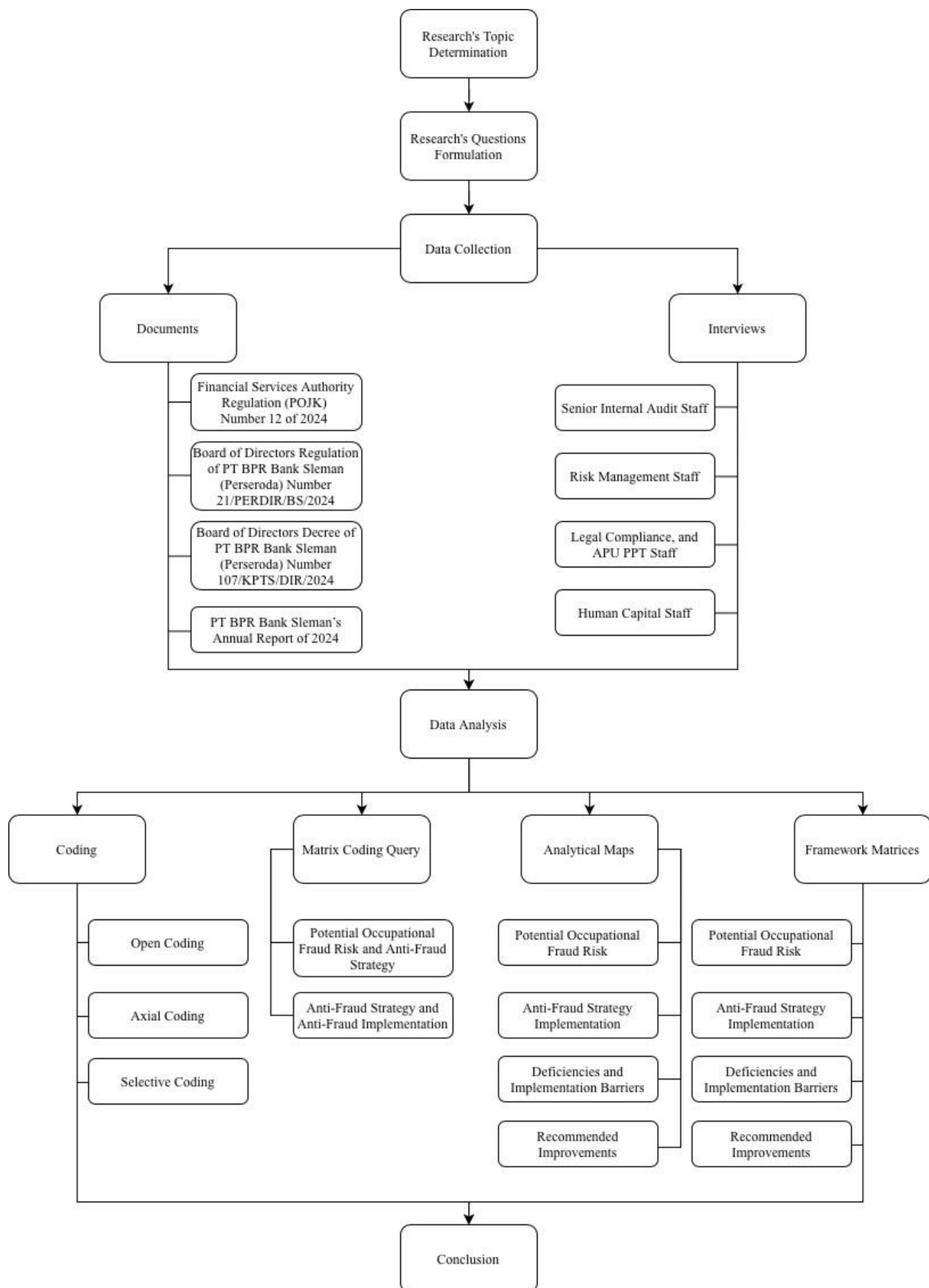


Figure 3.1 Research Systematics

3.5 Research Data Sources

The researcher collected data in this research through document analysis and interviews, both of which were aligned with the research objectives and research problems. To guarantee consistency and reliability, information gathered verbally from informants was cross-checked and supported by documents.

3.5.1 Documents

Documents are a valuable source of information in case study research, as they complement and strengthen findings derived from interviews. Documentary evidence provides contextual and factual support that enhances the validity of the analysis. Below are several documents utilized in this research:

1. Financial Services Authority Regulation (POJK) Number 12 of 2024 concerning the Implementation of Anti-Fraud Strategies for Financial Services Institutions;
2. Board of Directors Regulation of PT BPR Bank Sleman (Perseroda) Number 21/PERDIR/BS/2024 concerning the Anti-Fraud Strategy of PT BPR Bank Sleman (Perseroda);
3. Board of Directors Decree of PT BPR Bank Sleman (Perseroda) Number 107/KPTS/DIR/2024 concerning the Anti-Fraud Strategy Implementation Team of PT BPR Bank Sleman (Perseroda).
4. PT BPR Bank Sleman's Annual Report of 2024.

3.5.2 Interviews

Sekaran & Bougie (2016) stated that an interview is a purposeful and guided conversation conducted to obtain relevant information from individuals who possess knowledge about a particular issue. In research, interviews function as a primary data collection method that enables the researcher to explore informants' experiences, perceptions, and insights in depth. Interviews may be conducted face-to-face or through online media, and may take different forms depending on the objectives of the research.

Unstructured interviews are conducted without a fixed sequence of questions, allowing the researcher to begin with broad, open-ended inquiries to explore general issues and identify key themes for further investigation. This flexible approach enables participants to express their perspectives freely and helps the researcher gain a deeper understanding of the research context (Sekaran & Bougie, 2016). In contrast, structured interviews are used when the required information has been clearly identified. The questions are prepared in advance and arranged systematically, usually starting with an introduction that explains the interview's purpose and assures confidentiality. This is followed by a warm-up and main questions that are aligned with the research objectives, with probing questions used when further clarification or explanation is needed (Sekaran & Bougie, 2016).

In this research, both structured and unstructured interviews were employed. Structured interviews were conducted to obtain specific and

focused data in accordance with the research objectives and problem formulation, as several questions had been prepared in advance. At the same time, unstructured interviews were also applied when broad exploration was needed, particularly to gain a better understanding of the practical context and to identify key issues emerging from the field. In conducting the interviews, additional follow-up questions were asked based on the informants' responses whenever further clarification or deeper explanation was needed. The use of these two interview forms allowed the researcher to gather both targeted and exploratory data needed to answer the research questions. The informants interviewed in this research are as follows:

1. Mr. Arif Setiawan as Senior Internal Audit Staff.
2. Mr. Dwi Handoyo Miharjo as Risk Management Staff.
3. Mrs. Dian Chandra Dewi as Legal Compliance, and APU PPT Staff.
4. Mrs. Rizky Chitra as Human Capital Staff.

Table 3.1 Interviewee

Interviewee	Gender	Position	Years Worked (in Year)	Last Education	Age Group (in Year)
Mr. Arif Setiawan	Male	Senior Internal Audit Staff	12	Bachelor Degree in Agricultural Technology	40 - 45
Mr. Dwi Handoyo Miharjo	Male	Risk Management Staff	8	Master Degree in Accounting	30 - 35
Mrs. Dian Chandra Dewi	Female	Legal Compliance, and APU PPT Staff	7	Bachelor Degree in Law	30 - 35
Mrs. Rizky Chitra	Female	Human Capital Staff	10	Bachelor Degree in Psychology	35 - 40

3.6 Data Collection Method

The researcher employed data collection methods including interviews and document analysis. These methods significantly supported the completeness and reliability of the data gathered in answering the research problems. Specifically, the data collection process was carried out through the following approaches:

1. The researcher conducted interviews with several informants who represent the parties involved in the company's anti-fraud strategy team to obtain detailed information regarding the implementation of the anti-fraud strategy in minimizing occupational fraud at PT BPR Bank Sleman;

2. To complement the primary data, the researcher collected relevant documents related to the implementation of the anti-fraud strategy at PT BPR Bank Sleman to strengthen and validate the findings.

3.7 Data Analysis Method

This research applied qualitative data analysis to interpret the findings related to the research problems. There are generally three steps in qualitative data analysis, including data condensation, data display, and conclusion drawing (Miles et al., 2014). In this research, NVivo 15 software was used to support the analysis process by assisting the researcher in coding, managing, and systematically analyzing interview transcripts and documents. The software enabled the researcher to identify relationships across data sources, compare emerging themes, and maintain consistency throughout the coding process, lowering the potential for subjectivity and analytical bias. However, as the primary instrument in qualitative research, the researcher remains in full responsibility for the interpretation of the results as well as the development of the discussion and conclusions.

3.7.1 Coding

Qualitative research often produces a large volume of data, which requires the researcher to condense and organize the information through coding to generate more meaningful analytic units. Coding refers to the analytical procedure through which qualitative data are selected, focused, simplified, and integrated to develop meaningful interpretations and, ultimately, theoretical insights (Miles et al., 2014; Sekaran & Bougie, 2016). The primary objective of coding is to enable the researcher to draw

well-founded conclusions based on the analyzed data, by systematically labeling and organizing segments of data (Sekaran & Bougie, 2016).

According to Priyatni et al. (2020), the coding process was conducted using an inductive approach. The researcher thoroughly reviewed the data and subsequently developed a classification based on emerging patterns and themes. To ensure consistency and analytical clarity, specific coding criteria were carefully designed and applied throughout the data analysis process.

In the coding stage using NVivo 15, the researcher utilized interview data obtained from informants of PT BPR Bank Sleman along with relevant regulatory and internal documents concerning the implementation of the anti-fraud strategy, encompassing provisions on both the implementation team and strategic guidelines. These data were systematically organized into codes, which served as structured representations of key concepts emerging from the data. Each code incorporated relevant excerpts from interview transcripts and supporting documents, allowing the researcher to identify patterns and interpret relationships within the data.

The development of codes was aligned with the research questions, ensuring that each code directly corresponded to the formulated research problems. Moreover, relationships were established among conceptually related codes to illustrate analytical linkages. For example, codes related to potential fraud risk were connected to codes concerning Anti-Fraud

Strategy guidelines at PT BPR Bank Sleman. Through these analytical connections, the researcher was able to examine how identified fraud risks were addressed within the existing strategic framework of the bank.

3.7.2 Analytical Map

After completing the data condensation process through coding, the next step was data display. Referring to Miles et al. (2014), data display is a condensed and organized assembly of information that facilitates drawing conclusions and deciding on a response. Data visualisation in qualitative research helps the researcher in comprehending the data and determining whether additional analysis is required.

In this research, data presentation was carried out using analytical maps, matrix coding, and framework matrices generated through NVivo 15. Analytical maps were used as visual network displays to illustrate patterns, processes, and interrelationships among the codes. These maps were constructed by connecting codes with lines to represent analytical relationships (Miles et al., 2014). The codes reflected key concepts, categories, or themes identified in the data, while the connecting lines illustrated the relation between one another. In this research, the analytical maps were utilized to examine the mechanism of Anti-Fraud Strategy implementation, potential fraud risks, the alignment between identified risks and strategic guidelines, as well as challenges and improvement can be made in the implementation of the Anti-Fraud Strategy at PT BPR Bank Sleman.

3.7.3 Matrix Coding Query

Furthermore, the matrix coding query aims to support the researcher's explanation of the analysis of relationships among codes. According to Hai-Jew (2019), matrices are useful to explore and present data correlations and patterns in a structured form. Using this, the researcher analyzed whether certain concepts are related or meaningfully connected. In this research, matrix coding query applied to examine the relationship between potential occupational fraud and the anti-fraud strategy established at PT BPR Bank Sleman, as well as the relationship between the anti-fraud strategy and its implementation. Through the intersection of column and row, the researcher could identify the presence of these relationships across the coded data, leading to a clearer notice of how the codes were analytically related to one another (Hai-Jew, 2019).

3.7.4 Framework Matrices

The researcher then presented framework matrices in table form as part of the data presentation process. Framework matrices are qualitative analytical tools used to compare and summarize research data from various sources, such as interviews, documents, and observations (Miles et al., 2014). In this research, the framework assisted the researcher to better comprehend the codes created during analysis and the coding results obtained from interview data with PT BPR Bank Sleman informants. Additionally, case categories were developed to preserve interview transcripts and to separate participant responses from interviewer

questions. As tabular displays, framework matrices arranged data in one place for easier viewing and detailed analysis, allowing the researcher to compare code across different sources and examine whether similar findings appeared across multiple informants and documents (Miles et al., 2014). In this way, the framework matrices supported source triangulation and strengthened the analytical process by making it easier to find patterns, relationships, and consistency within the research data.

3.7.5 Conclusions

The final phase in the qualitative data analysis is conclusion drawing and verification (Miles et al., 2014). During this process, the researcher must interpret the findings carefully and accurately to ensure analytical integrity. Miles et al. (2014) stated that qualitative conclusions emerge throughout the analysis by identifying patterns, relationships, explanations, and propositions and are continuously verified to ensure data validity. The final conclusions regarding the studied topic were further formulated by the researcher based on the data that had been collected and systematically analyzed. Accordingly, the research problems posed at the beginning of the study should be explicitly addressed and clearly answered in a solid conclusion.

3.8 Data Validity Test

This research applied a number of qualitative data validation procedures notably, triangulation, regular debriefing sessions, and persistent observation, to guarantee the reliability and validity of the findings. The fundamental idea behind

triangulation is that greater confidence in research findings can be achieved when various approaches or sources produce consistent findings. To perform triangulation, a research problem must be studied from several perspectives (Sekaran & Bougie, 2016). By this, researchers can finally obtain a higher degree of accuracy and credibility (Olsen, 2004). Additionally, Miles et al. (2014) described triangulation involves the use of multiple sources and modes of evidence to verify findings and to examine a phenomenon from different perspectives. In this way, triangulation helps strengthen the trustworthiness of the analysis and reduce the possibility of bias during data collection and analysis.

Sekaran & Bougie (2016) outlined that triangulation can be categorized into four main types. First, method triangulation refers to the use of multiple data collection or analysis methods within the research. Second, source triangulation entails obtaining information from multiple sources or at various times to improve consistency. Third, researcher triangulation, which reduces individual bias by involving numerous researchers in data collection or analysis. Lastly, theory triangulation comprises interpreting and explaining research findings using various theoretical perspectives.

The triangulation techniques applied in this research are as follows:

1. Source Triangulation

Source triangulation was conducted by collecting data from multiple parties engaged in the implementation of the PT BPR Bank Sleman's Anti-Fraud Strategy.

2. Method Triangulation

Method triangulation was conducted by examining data obtained from the same organizational units using different data collection methods. Interviews and document analysis of pertinent internal and regulatory policies pertaining to the anti-fraud strategy were integrated in this research. By using this approach, the researcher was able to verify information and make sure that spoken claims and written proof were consistent.

In addition to triangulation techniques, persistent observation was also applied in this research. According to Korstjens & Moser (2018), this involved continuous engagement with the data through repeated reading, coding, recoding, relabelling, and category refinement until adequate analytical depth is attained. To thoroughly assess the consistency, relevance, and interpretation of the data in this study, the researcher repeatedly reviewed interview transcripts and supporting documents. Through this procedure, the researcher was able to concentrate more intently on significant categories, improve codes as needed, and make sure that the findings were not based on a cursory reading or shallow interpretation. Persistent observation ultimately enabled the researcher to gain a deeper comprehension of the facts and generate conclusions that were more grounded in the collected evidence.

Regular debriefing sessions were another method carried out between the researcher and the research supervisor. Shenton (2004) explained that such sessions provide an opportunity for the researcher to discuss alternative

approaches, test developing interpretations, and receive critical feedback from others in a supervisory capacity. In this research, these discussions served as an evaluative procedure that allowed the researcher to reexamine coding decisions, reconsider preliminary interpretations, and identify possible weaknesses in the analytical approach. Feedback from the supervisor also helped the researcher to recognize personal assumptions or preferences that might affect the data interpretation. Therefore, regular debriefing sessions did not merely function as formal supervision but also strengthened the findings' legitimacy and analytical rigor.

Finally, NVivo 15 was utilized to support data validation and analytical rigor. The software improved consistency, traceability, and transparency throughout the qualitative analysis process by enabling a feasible connecting process between coded data and analytical categories, and systematically arranging interview sources and documents.

CHAPTER IV

DATA PRESENTATION AND DISCUSSION

This chapter presents the findings of the research conducted at PT BPR Bank Sleman regarding the implementation of the anti-fraud strategy in minimizing occupational fraud. The first section of this chapter will discuss the profile of PT BPR Bank Sleman. The researcher then discusses the responses to the formulated research questions based on the information gathered from interviews and documents obtained. Finally, based on the interviews' findings, the author concludes by offering recommendations for resolving challenges in implementing anti-fraud strategies into practice to reduce occupational fraud.

4.1 Profile of PT BPR Bank Sleman

4.1.1 History of PT BPR Bank Sleman

PT BPR Bank Sleman (Perseroda), or widely known as Bank Sleman, is a regionally owned enterprise of the Government of Sleman Regency. Currently, its share ownership consists of 99.5% held by the Government of Sleman Regency and 0.50% held by Koperasi Pegawai Republik Indonesia-Koperasi Pegawai Kabupaten Sleman (KPRI-KP2KS). As a regionally owned enterprise, Bank Sleman plays a role in supporting the regional economy, particularly through financing for micro, small, and medium enterprises (MSMEs). In its business activities, Bank Sleman operates in the banking services sector with main products consisting of savings, deposits, and loans.

Historically, Bank Sleman was established under the Regional Regulation of Sleman Regency Number 3 of 1962, 19th May 1962, concerning the establishment of a market bank, and the Recent Decree of Sleman Number 3/K/970 dated 24th March 1970 concerning the implementation guidelines for the regional market bank of Sleman Regency. Since 1970, the Bank has been operating in the banking sector under its original name, *Bank Pasar*.

As the business developed, a Temporary Articles of Association for the Regional Company “*Bank Pasar*” of Sleman Regency was issued through the Decree of the Regent of Sleman Number 076/Kep.KDH/1981 on 21st July 1981. This temporary statute was later refined by the Regional Regulation of Sleman Regency Number 15 of 1983 on 21st June 1983, which was subsequently approved by the Governor of the Special Region of Yogyakarta through Decree Number 209/KPTS/1983 on 21st November 1983. Additionally, the Bank obtained its business license from the Ministry of Finance of the Republic of Indonesia through Letter Number S-387/MK.11/1981 on 28th November 1981.

A further legal transformation took place based on the Regional Regulation of Sleman Regency Number 30 of 1995 on 6th September 1995, which was approved by the Governor of the Special Region of Yogyakarta via Decree Number 95/KPTS/1996 on 15th April 1996. Through this change, the legal form of the institution became PD Bank Perkreditan Rakyat “*Bank Pasar*” Kabupaten Dati II Sleman. Later, in 2008, another

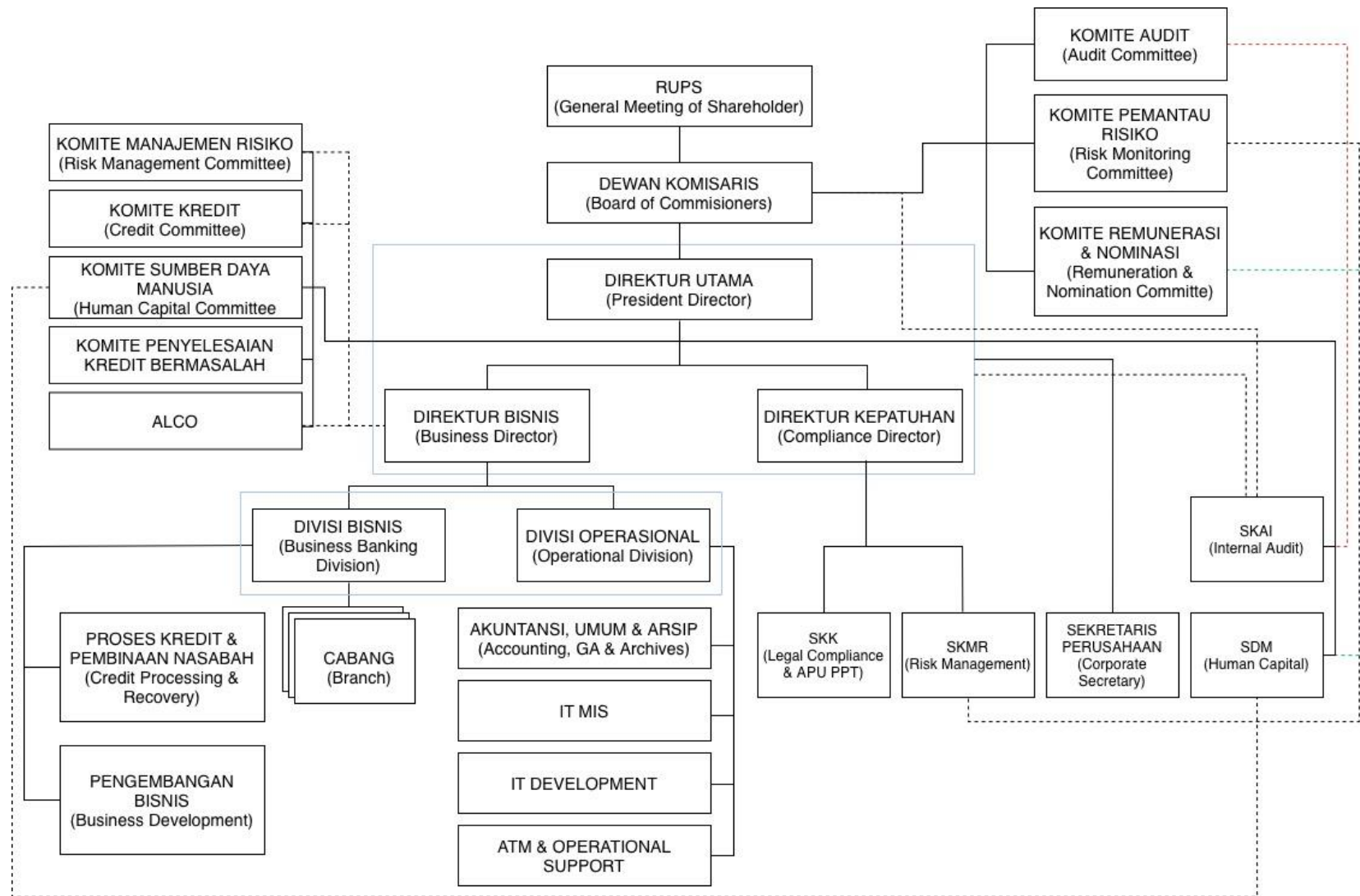
change was made through the Regional Regulation of Sleman Regency Number 2 of 2008 concerning the Regional Rural Bank of Bank Sleman. Since then, the Bank's name changed to PD BPR Bank Sleman. This change also received approval from the Bank Indonesia through the Decree of the Head of Bank Indonesia Yogyakarta Number 10/2/KEP.PBI/Yk/2008 on 18th February 2008.

In its subsequent development, the legal framework governing Bank Sleman was amended again in 2013 through the Regional Regulation of Sleman Regency Number 20 of 2013, which revised the Regional Regulation Number 2 of 2008. One of the important points in this amendment was the clarification that the capital of Bank Sleman originated from regional Government equity participation, with regional capital amounting to IDR 110 billion. Furthermore, through the Regional Regulation of Sleman Regency Number 6 of 2016 concerning the Second Amendment to the Regional Regulation Number 2 of 2008, the authorized capital of Bank Sleman was set at IDR 230 billion.

In line with the increasingly competitive development of the banking industry, Bank Sleman later transformed into PT BPR Bank Sleman (Perseroda). This change in legal form was based on the Regional Regulation of Sleman Regency Number 2 of 2019 concerning the conversion of the legal entity from a Regional Rural Bank Company into a Limited Liability Company of PT BPR Bank Sleman (Perseroda). This provision was further formalized in Notarial Deed of Hitaprana, S.H.

Number 5 of 2019 concerning the establishment of PT BPR Bank Sleman (Perseroda), and was reinforced by the Decree of the Board of Commissioners of the Financial Services Authority (OJK) Number KEP-110/KO.031/2019 concerning the transfer of the business license from PD Bank Perkreditan Rakyat Bank Sleman to PT Bank Perkreditan Rakyat Bank Sleman (Perseroda). Accordingly, since 2020, the Bank has officially operated under the name PT BPR Bank Sleman (Perseroda).

4.1.2 Organizational Structure of PT BPR Bank Sleman

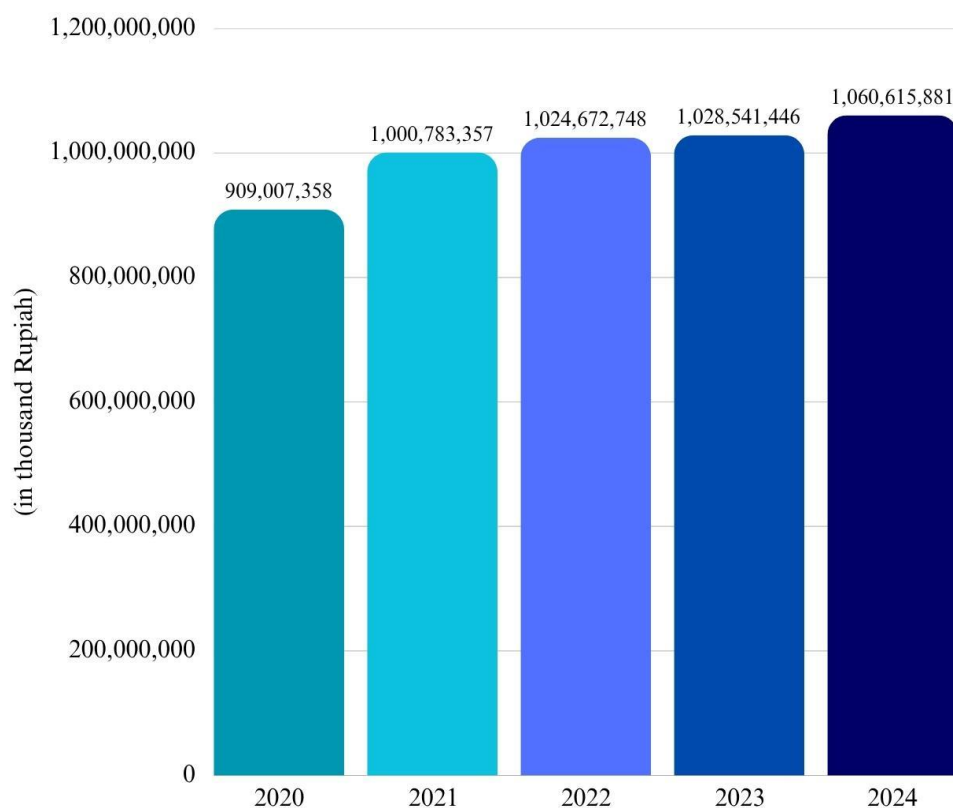


Source: PT BPR Bank Sleman

Figure 4.1 Organizational Structure of PT BPR Bank Sleman

4.1.3 Financial Profile of PT BPR

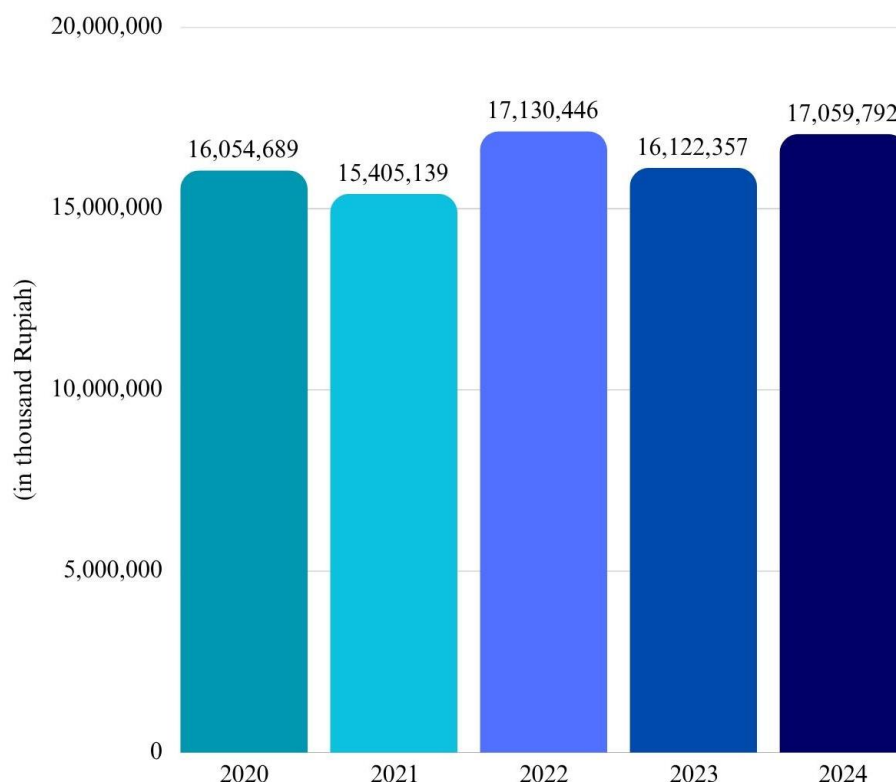
PT BPR Bank Sleman exhibits a relatively substantial financial scale for a local rural banking organization. It is a regionally owned rural bank with a long institutional history that focuses on savings, deposits, loans, and supporting banking services. The Bank's financial profile is important to describe because it provides a clearer picture of its operation scope, the extent of its financial capacity, and the strength of its intermediation role in supporting the community, especially in Sleman Regency. Based on the five-year financial data from 2020 to 2024, the Bank has maintained positive profitability while exhibiting constant growth in assets and loans during the observed period.



Source: PT BPR Bank Sleman

Figure 4.2 Total Assets of PT BPR Bank Sleman Year 2020-2024

The preceding figure shows that PT BPR Bank Sleman's assets increased from IDR 909 billion in 2020 to IDR 1.06 trillion in 2024. The increase occurred gradually throughout the observed years. This trend indicates that the Bank has continued to expand its financial base over time. In the rural bank context, the growth in total assets reflects an increasing scale of operations and shows that the Bank has maintained its capacity to support its main products and services, particularly fund-raising and lending activities.

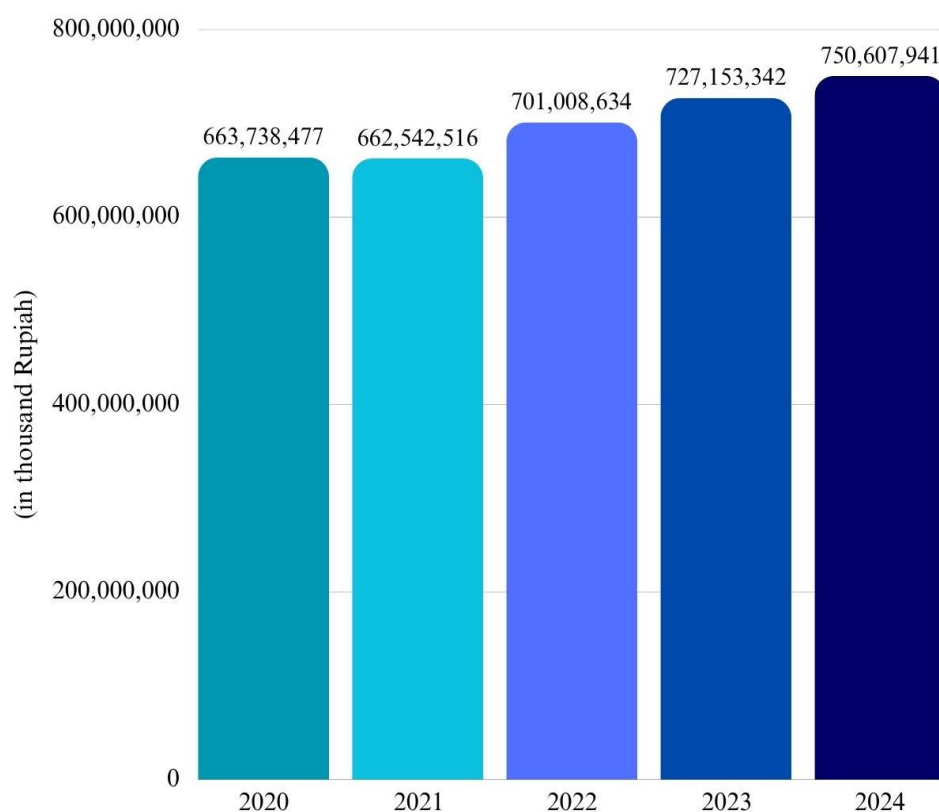


Source: PT BPR Bank Sleman

Figure 4.3 Net Profit of PT BPR Bank Sleman Year 2020-2024

Besides, PT BPR Bank Sleman also maintained positive net profit throughout the 2020 to 2024 period, although it fluctuated slightly from year to year, as shown in the graph above. Net profit stood at IDR 16.05 billion in 2020, decreased to IDR 15.41 billion in 2021, rose to IDR 17.13 billion in 2022, declined slightly to IDR 16.12 billion in 2023, and increased again to IDR 17.06 billion in 2024. These illustrate that the Bank was able to remain profitable across the observed period. This condition describes that, despite fluctuations, PT BPR Bank Sleman has maintained its ability to generate earnings from its banking operations and sustain its business continuity.

Figure 4.4 Loans Outstanding of PT BPR Bank Sleman Year 2020-2024

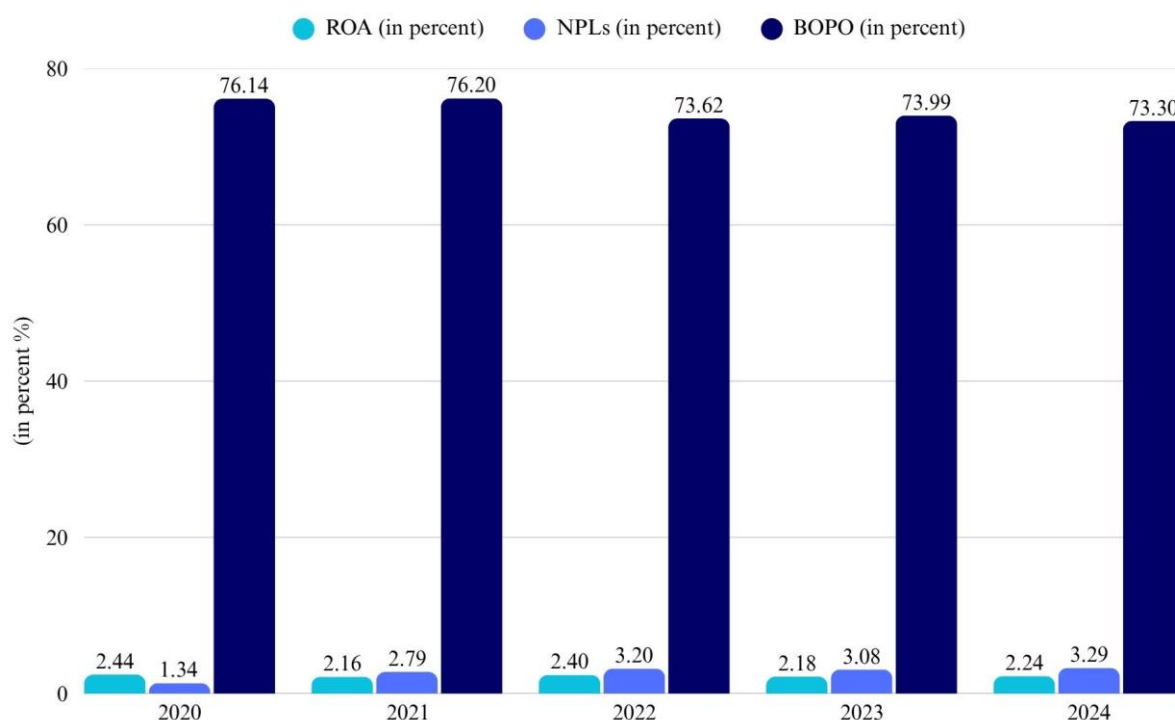


Source: PT BPR Bank Sleman

Figure 4.4 Loans Outstanding of PT BPR Bank Sleman Year 2020-2024

As the graph above illustrates, the amount of outstanding loans indicates that lending is still one of PT BPR Bank Sleman's primary functions. In 2020, the total amount of outstanding loans was IDR 663.74 billion; by 2021, that amount had somewhat decreased to IDR 662.54 billion. Following that, the amount rose to IDR 701.01 billion in 2022, IDR 727.15 billion in 2023, and IDR 750.61 billion in 2024. This increasing pattern shows that the Bank's lending operation kept expanding, particularly after 2021. This development illustrates the Bank's ongoing involvement in directing funds to the community and supporting its

intermediation function as a rural bank, given that credit products are one of the Bank's primary offerings.



Source: PT BPR Bank Sleman

Figure 4.5 Ratio Trends of PT BPR Bank Sleman Year 2020-2024

In the figure above, ROA remained relatively stable during the observed period, ranging from 2.16% to 2.44%. It indicated that the Bank was able to maintain a fairly consistent level of profitability in relation to its assets. Meanwhile, the NPL ratio increased from 1.34% in 2020 to 3.29% in 2024. Although it remained below 5% across the observed period, it still suggests that the Bank's credit quality was relatively maintained despite the increase in loans outstanding over time. In addition, the BOPO ratio fluctuated within a relatively narrow range, from 73.30% in 2024 to 76.20% in 2021. This explains that PT BPR Bank Sleman maintained a fairly stable level of operational efficiency, although operational costs still

accounted for a considerable portion of operating income. Within this data, the ratio patterns prove that the Bank was able to preserve profitability, manage credit risk, and maintain relatively steady efficiency from 2020 to 2024.

4.1.4 Products and Services of PT BPR Bank Sleman

In its development, PT BPR Bank Sleman has continuously sought to respond to the financial needs of the community, particularly those of Sleman Regency. As a regionally owned rural bank, Bank Sleman places emphasis on providing accessible and reliable banking services while also supporting local economic development, especially through financing for micro, small, and medium enterprises (MSMEs). In general, the products and services offered by the Bank Sleman can be grouped into three main categories, namely fund-raising products, lending products, and banking services and digital solutions.

Bank Sleman provides a variety of time deposits and savings products as fundraising options. Its savings products include Tabungan Mutiara, Tabungan Bank Sleman, Tabungan SimPel, Tabungan Arofah, Tabungan Tamasya Plus, TabunganKu, and Tabungan Pensiun. Additionally, the bank provides a deposit product called Deposito Berlian. These items show that Bank Sleman offers solutions designed for various customer segments and financial goals in addition to general savings facilities. Besides, Bank Sleman provides several credit facilities designed to accommodate both personal and business needs. The current lending

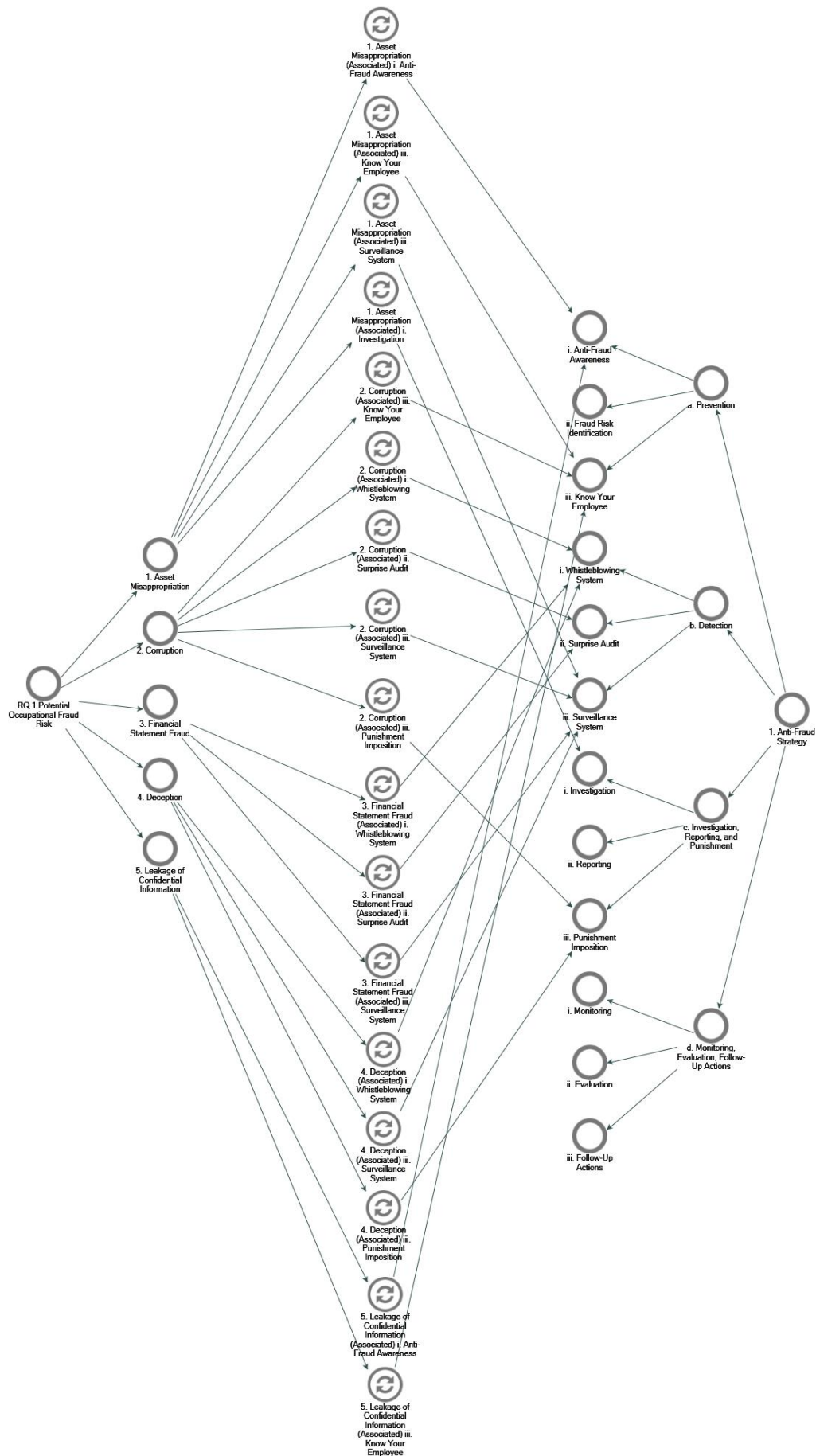
products include Kredit Konsumtif Kolektif, Kredit Konsumtif Personal Loan, Kredit Usaha, Kredit Linkage, and Kredit Air Bersih dan Sanitasi (Kasih Sembada).

In addition to the products mentioned above, Bank Sleman provides supporting banking services and digital solutions to facilitate customer transactions. ATM Silver and ATM Gold are two of its ATM services. While the Gold card offers comparable features with a greater daily transaction limit, the Silver card facilitates typical ATM transactions, including balance inquiries, cash withdrawals, transfers to other Bank Sleman accounts, and transfers to other banks. On top of that, Bank Sleman delivers a number of digital options, such as mobile collection, virtual accounts, e-statements, and WhatsApp notifications. In keeping with the growing usage of digital service channels, the bank's efforts to enhance transaction convenience and offer more useful banking support are reflected in these services.

4.2 Types of Occupational Fraud Potential at PT BPR Bank Sleman

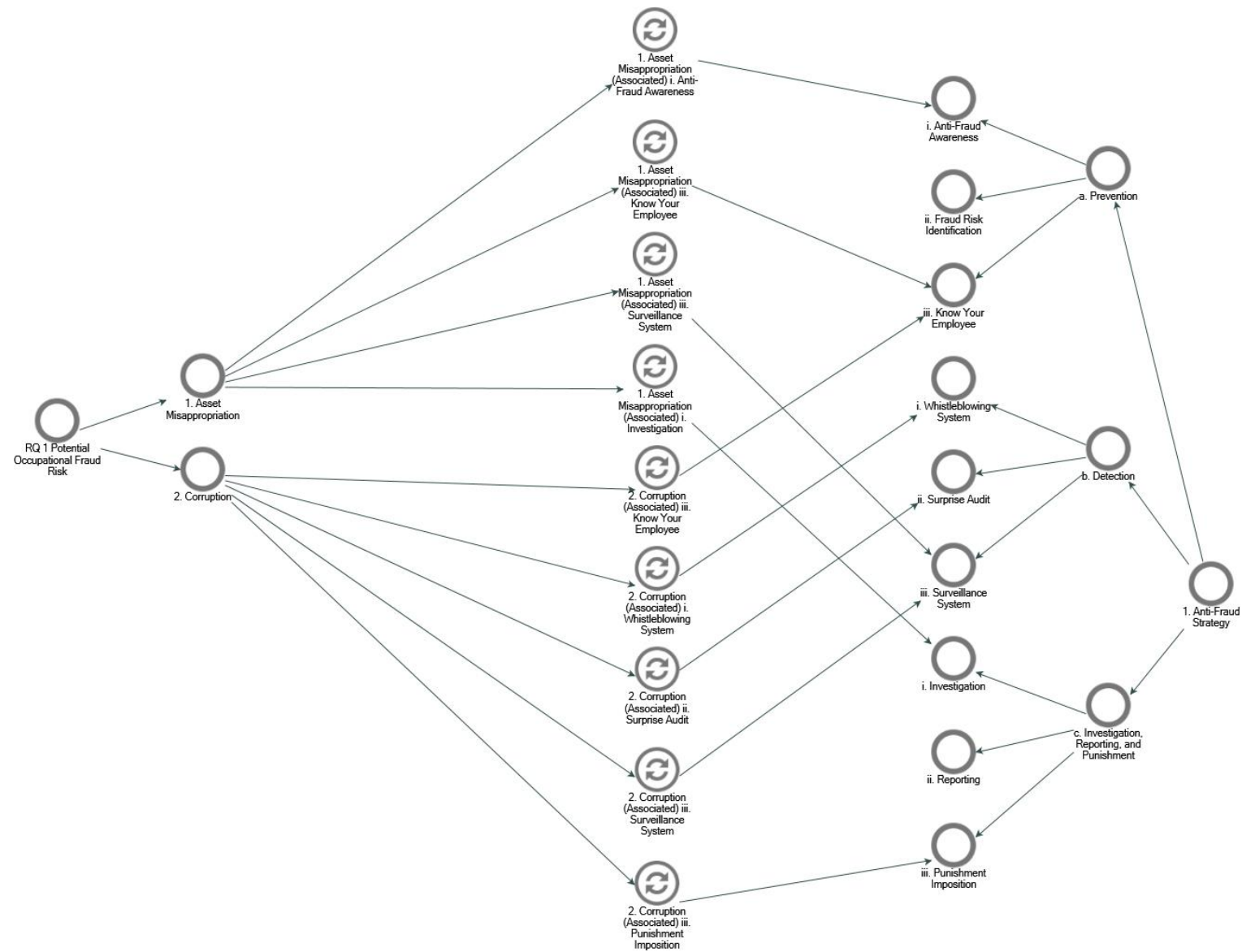
The occupational fraud risks in the operational environment of PT BPR Bank Sleman can be classified into five main categories, namely asset misappropriation, corruption, financial statement fraud, deception, and leakage of confidential information. These categories are identified from the interview data. They are also clearly stated in the Guideline for the Implementation of Anti-Fraud Strategy of PT BPR Bank Sleman, particularly in Chapter 2 on anti-fraud

management. To provide a better overview of these categories, the results of the NVivo analysis are presented in the figure below.



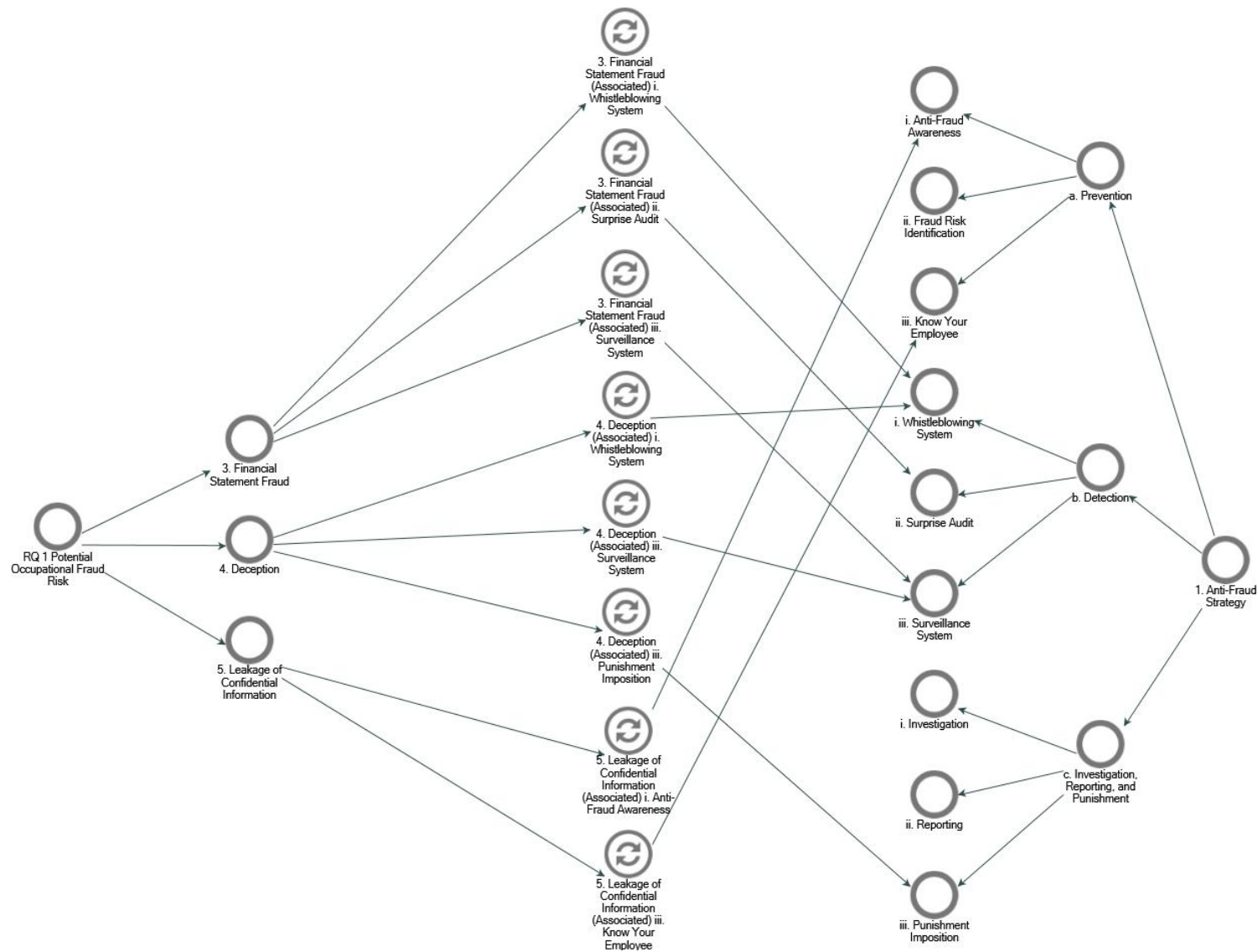
Source: Analyzed by The Researcher using NVivo 15

Figure 4.6 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman



Source: Analyzed by The Researcher using NVivo 15

Figure 4.7 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman Focused on Asset Misappropriation and Corruption



Source: Analyzed by The Researcher using NVivo 15

Figure 4.8 Analytical Map of Potential Occupational Fraud at PT BPR Bank Sleman Focused on Financial Statement Fraud, Deception, and Leakage of Confidential Information

	1. Anti-Fraud Strategy	a. Prevention	i. Anti-Fraud Awareness	ii. Fraud Risk Identification	iii. Know Your Employee	b. Detection	i. Whistleblowing System	ii. Surprise Audit	iii. Surveillance System
RQ 1 Potential Occupational Fraud Risk	No	No	No	No	No	No	No	No	No
1. Asset Misappropriation	No	No	Yes	No	Yes	No	No	No	Yes
2. Corruption	No	No	No	No	Yes	No	Yes	Yes	Yes
3. Financial Statement Fraud	No	No	No	No	No	No	Yes	Yes	Yes
4. Deception	No	No	No	No	No	No	Yes	No	Yes
5. Leakage of Confidential Information	No	No	Yes	No	Yes	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.9 Matrix Coding of Potential Occupational Fraud at PT BPR Bank Sleman

	c. Investigation, Reporting, and Punishment	i. Investigation	ii. Reporting	iii. Punishment Imposition	d. Monitoring, Evaluation, Follow-Up Actions	i. Monitoring	ii. Evaluation	iii. Follow-Up Actions
RQ 1 Potential Occupational Fraud Risk	No	No	No	No	No	No	No	No
1. Asset Misappropriation	No	Yes	No	No	No	No	No	No
2. Corruption	No	No	No	Yes	No	No	No	No
3. Financial Statement Fraud	No	No	No	No	No	No	No	No
4. Deception	No	No	No	Yes	No	No	No	No
5. Leakage of Confidential Information	No	No	No	No	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.9 Matrix Coding of Potential Occupational Fraud at PT BPR Bank Sleman

4.2.1 Asset Misappropriation

Asset misappropriation refers to an unlawful act committed for personal or other improper benefit by misusing the Bank's assets or assets owned, managed, or controlled by the Bank without following the applicable procedures, thereby causing actual or potential loss to the Bank (PT BPR Bank Sleman, 2024). The Bank's guideline for anti-fraud strategy implementation shows that this category includes misuse of inventory and other assets in addition to cash. Unauthorized disbursement, cash theft, and embezzlement of pension benefits, guarantee funds, and claim cash are all covered under the guidelines. It also extends to the misuse of theft or improper use of inventory and other asset accounts, such as their use as a source of installment payments or employee purchases. Viewed in this way, Dwi Handoyo Miharjo (2025), representing Risk Management staff, explained that asset misappropriation concerns the use of assets under the Bank's control for personal benefit in ways that may harm the Bank.

In practice, the strongest exposure appears in the handling of customer funds. Arif Setiawan (2026), Senior Internal Audit staff, stated that internal fraud may involve both failing to deposit money that has already been received and embezzling customer funds through unauthorized withdrawals. This demonstrates the direct connection between asset misappropriation at PT BPR Bank Sleman and circumstances in which funds under the bank's control are taken out without proper

authorization or obtained from clients but not properly restored to the formal banking procedure.

The same vulnerabilities also arise in daily banking activities involving direct access to money. Miharjo (2026) explains that funds disbursed through the credit process may be exploited, while the same risk is also present in delivery service and pick-up service activities, where employees physically handle customer funds outside regular counter-based transactions. In these activities, weak employee integrity may lead to the misuse of collected or delivered funds and to those funds not being deposited into the Bank. This concern is further reinforced by the Bank's emphasis on employee background and financial behavior. Rizky Chitra (2025), as Human Capital staff, noted that checking employee SLIK and OJK SIPELAKU is considered effective because it can reveal lifestyle patterns and loan obligations, as well as determine whether a candidate has engaged in fraud in the past.

Further indications of this risk can be seen in work units that directly manage customer funds. Miharjo (2026) referred to physical cash discrepancies, particularly in teller activities, where shortages or inexplicable variances may point to irregularities in the funds handling. Dian Chandra Dewi (2025), as Legal Compliance, and APU-PPT Department staff, likewise identified funding, lending, credit, and teller as the units most exposed to this risk, as they meet with clients on a daily basis and carry direct responsibility for managing clients' funds, which leads to

familiarity. Given this level of exposure, the operational chain pertaining to customer funds is accompanied by several controls, such as transaction recording, superior approval, confirmation, and system-based safeguards like CCTV, fraud detection systems, and audit trails (Dewi, 2025). The presence of these controls indicates that the Bank has recognized these functions as particularly vulnerable to misuse.

4.2.2 Corruption

PT BPR Bank Sleman (2024) stated that corruption is associated with the misuse of influence, position, or authority for improper benefit in ways that may directly or indirectly, both benefit and/or harm clients, the Bank, or other parties. It comprises conflict of interest, bribery, illegal acceptance, and extortion, which reflects the understanding that fraud is not limited to theft alone and that conflict of interest is already inclusive (Dewi, 2026; Miharjo, 2025; PT BPR Bank Sleman, 2024). More specifically, this category also includes practices such as granting lower interest rates to shareholders outside applicable procedures, hiring employees due to personal ties rather than competence, bribing third parties for licensing matters, money, goods, or other benefits so that a credit application is approved, receiving personal commissions from credit disbursement and interest, selling foreclosed assets at an unreasonable price for personal gain, and requesting money from debtors to obtain a special deposit rate (PT BPR Bank Sleman, 2024).

This risk is further reflected in the way internal authority may be used beyond proper procedure. The approval of problematic credit due to a conflict of interest is one example, with other indications including staff collusion to hide irregularities and the falsification of internal documents such as signatures and transaction evidence (Setiawan, 2026). Miharjo (2026) referred that more specific exposure appears in the credit disbursement process, where gratification, rewards, or other benefits outside banking regulations may be received once credit has been granted. The fact that this stage is followed by direct confirmation with clients and system-based checks indicates that it is seen as particularly vulnerable to inappropriate benefit arising from the abuse of authority.

Corruption is not confined to the credit stage. It may also arise through cooperation between superiors and subordinates in carrying out fraud, which explains why employee rolling is applied periodically, especially in vulnerable positions (Miharjo, 2026). The same conditions can also be seen in procurement activities, where corruption shows as bribery or reward from business partners, mark-up pricing, fake vendors, and procurement that deviates from specifications (Chitra, 2026; Setiawan, 2026). These patterns imply that corruption may encompass the abuse of power, coordinated attempts to shield improper decisions, and dealings with external parties, whereas personal gain may override procedure and institutional needs in addition to direct financial transactions.

4.2.3 Financial Statement Fraud

Dewi (2026) identified financial reporting fraud as one of the fraud potentials faced by PT BPR Bank Sleman. It is reflected in reporting and finance-related misconduct such as the concealment of problematic credit or non-performing loans (NPL), financial statements manipulation, and provisions for impairment losses exploitation. These forms convey that the issue does not lie merely in inaccurate reporting, but in the intentional manipulation of financial data to misrepresent the Bank's true state. The quality of the Bank's assets and the picture of its financial performance may be distorted due to concealed bad credit and manipulated provisions (Chitra, 2026; Setiawan, 2026).

Referring to PT BPR Bank Sleman (2024), financial statement fraud itself is defined as the intentional misstatement or omission of amounts or disclosures in financial reports, including off-balance sheet items, in ways that are inconsistent with generally accepted accounting practices and designed to benefit the perpetrator or harm customers, the Bank, and/or other parties. This category is placed into two broad forms, namely the overstatement and the understatement of net assets or net income. Overstatement may occur through mismatches in the timing of bookkeeping, inaccurate revenue recognition, inability to disclose liabilities and expenses, improper asset valuation and disclosure, while understatement may arise through similar irregularities in bookkeeping and revenue recognition, the overstatement of liabilities and expenses, and

further inaccuracies in asset valuation and disclosure (PT BPR Bank Sleman, 2024).

4.2.4 Deception

According to Setiawan (2026), deception may arise when false information, manipulated documents, and deceptive tactics are used to make irregular activities seem valid or legitimate. This is evident in the credit process, where lending decisions may be supported by falsified debtor data, marked-up collateral, fictitious credit, dishonest debtors, and forged supporting documentation. The same tendency is noticed in fictional or nominee debtors, engineered credit analysis incorporating BI Checking, SLIK, and cash flow, over-financing, and collateral values that do not match actual conditions (Chitra, 2026; Setiawan, 2026).

This extends further into digital transactions, making irregular activities appear as ordinary customer behavior. Such cases include ATM transactions carried out simultaneously within a short time span, transactions conducted by non-customers, and passive accounts that are still able to perform transactions, all of which are treated as abnormal by the Fraud Detection System to identify potential fraud at an early stage (Miharjo, 2026). Dewi (2025) also pointed out that ATM and virtual account transactions taking place far from Bank Sleman, as well as repeated transactions at different ATMs over long distances, may be automatically rejected by the system since they appear to be suspicious activity. When a transaction is classified as a red flag or treated as abnormal by the FDS,

further verification is carried out to determine whether it was genuinely performed by the customer or whether the card or account may already have been compromised or hacked, in which case replacement and additional action may be required.

These forms of deception are aligned with statement by PT BPR Bank Sleman (2024), which defines deception as behavior intended to gain advantage or prevent loss through manipulation, misleading actions, false representations, or other forms of deceit in relation to Bank Products, services, transactions, market conditions, or prices. Additionally, it is illustrated by promises that do not match actual conditions, fictitious debtors or credit given under false identities, nominee debtors with real identities but whose money is used by third parties, and the manipulation of credit documents. The significance of this category is demonstrated by the penalties meted out to employees who commit fraud or deception, such as a penalty, demotion, or termination of employment (Chitra, 2025). Collectively, deception at PT BPR Bank Sleman is associated with fabricated debtor information, manipulated documentation and assessments, fraudulent procurement arrangements, and suspicious digital transactions that resemble legitimate activity.

4.2.5 Leakage of Confidential Information

Leakage of confidential information is also recognized as one of the fraud potentials faced by PT BPR Bank Sleman (Dewi, 2026). This exposure is not confined to financial loss alone, but also concerns the

security of data and confidentiality attached to banking activities. As noted by Miharjo (2025), fraud is understood to extend beyond the misuse of money to include the leakage of data and confidential information, which places this issue within the area of fraud that should be recognized across all work units rather than by one division alone.

PT BPR Bank Sleman (2024) frames this category explicitly in the Bank's guideline for anti-fraud strategy implementation, as the unlawful dissemination of confidential information belonging to the Bank and/or other parties to persons who have no authority to receive it, in ways that may benefit or harm customers, the Bank, or other parties. More specifically, it includes the provision of third-party data to unauthorized persons and the disclosure of customer data or activities to parties without authority unless written consent has been obtained or disclosure is required by law. In more concrete terms, the risk appears in information technology fraud such as illegal access to the banking system, misuse of employee user IDs and passwords, and manipulation of transaction data in the system (Chitra, 2026; Setiawan, 2026).

The way the system is designed and monitored further highlights this vulnerability. Access is structured through verification, dual control, and double checking rather than being placed under single authorization alone, while audit trails are employed to record who accessed the system, when access occurred, what was accessed, what was downloaded, and what changes were made. Suspicious transaction analysis is conducted both

through the Fraud Detection System and outside it, using pre-determined indicators to assess whether the transaction activity is abnormal, while CCTY forms part of the wider oversight surrounding fraud detection (Dewi, 2025; Miharjo, 2026). Although these mechanisms function as controls, they demonstrate how closely this risk is tied to access rights, system activity, and the possibility that confidential data may be viewed, used, downloaded, or altered by unauthorized parties.

4.3 Anti-Fraud Strategy Implementation

In implementing its anti-fraud strategy, PT BPR Bank Sleman has formally established an Anti-Fraud Strategy team through the Director's Decree Number 107/KPTS/DIR/2024, which regulates the team's formation, roles, and responsibilities (PT BPR Bank Sleman, 2024). On top of that, PT BPR Bank Sleman has also established its own internal guideline referred to the Board of Directors Regulation Number 21 of 2024 concerning the Guidelines for the Implementation of the Anti-Fraud Strategy of PT BPR Bank Sleman (Perseroda). Under this regulation, the anti-fraud strategy is structured as a comprehensive fraud control system consisting of four interrelated pillars. These pillars comprise (1) Prevention; (2) Detection; (3) Investigation, Reporting, and Punishment; (4) Monitoring, Evaluation, and Further Action. Through this structure, the anti-fraud strategy implementation at PT BPR Bank Sleman is not limited to responding to fraud after it occurs, but is arranged as an integrated mechanism that begins with preventive efforts, continues with detection and case handling, and is followed by monitoring, evaluation, and corrective actions to strengthen internal control and

minimise the recurrence of similar fraud incidents, in accordance with POJK Number 12/2024 concerning the Implementation of Anti-Fraud Strategy for Financial Services Institutions. This four-pillar structure is further demonstrated by NVivo analysis shown in the next figure.

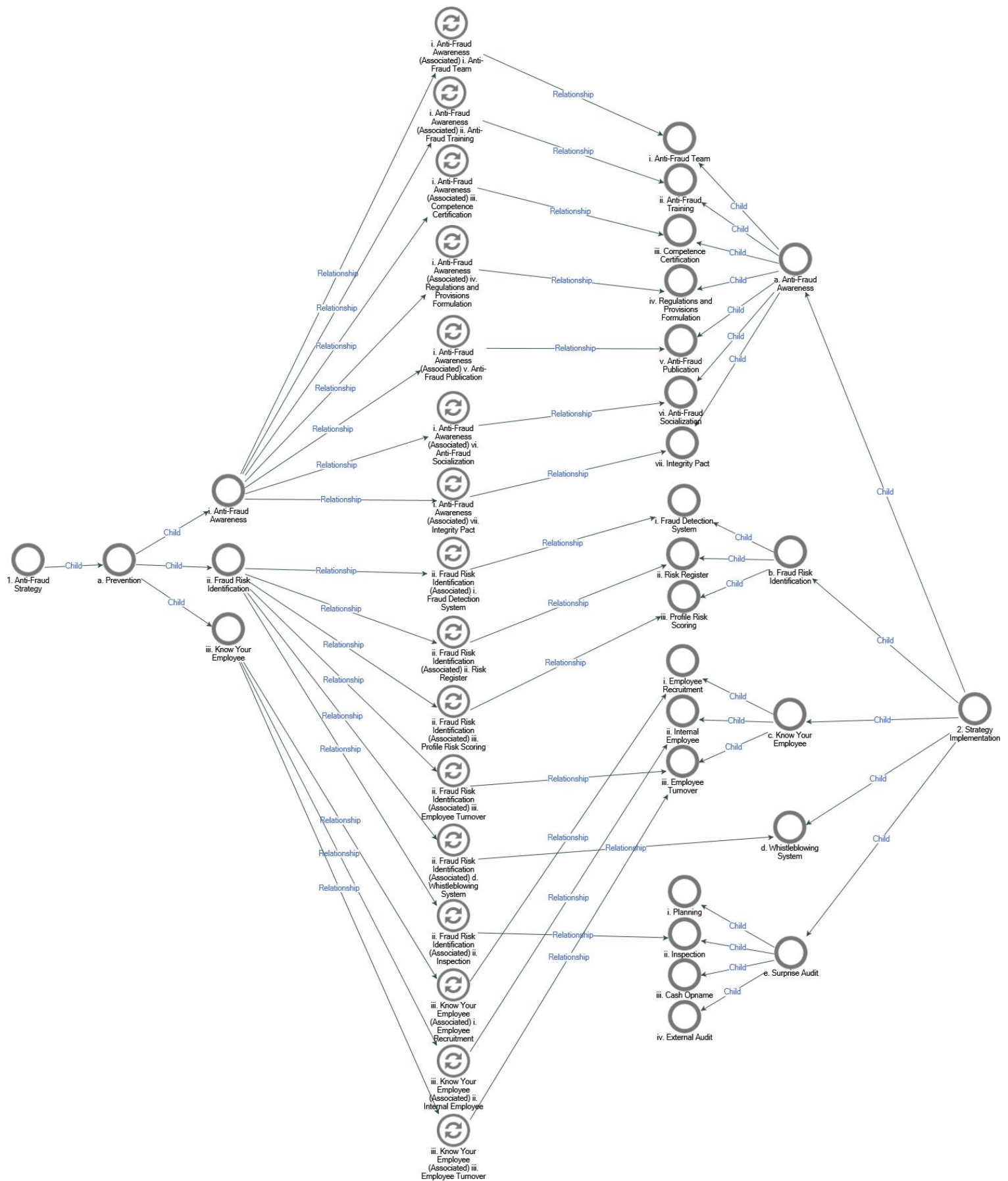
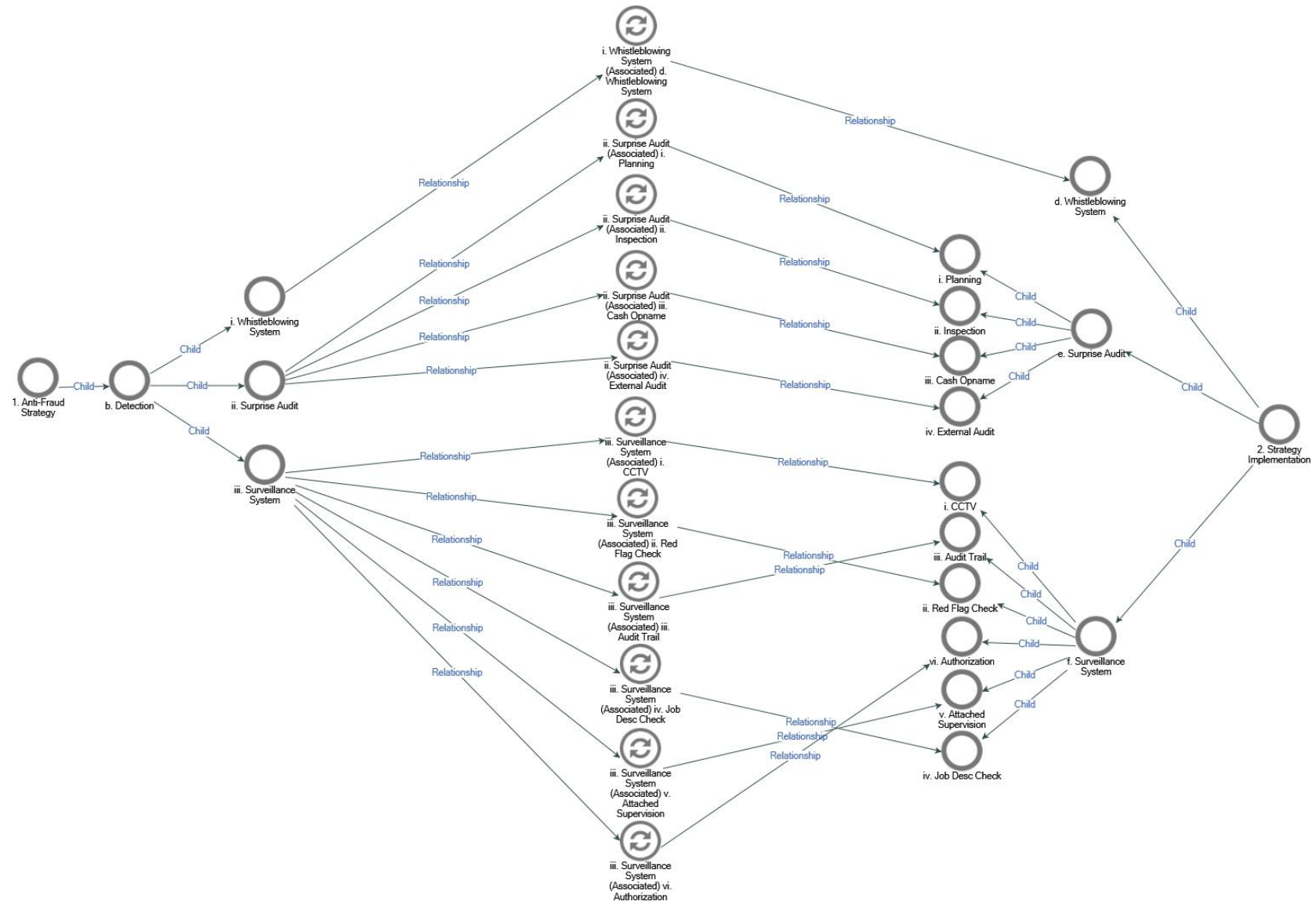
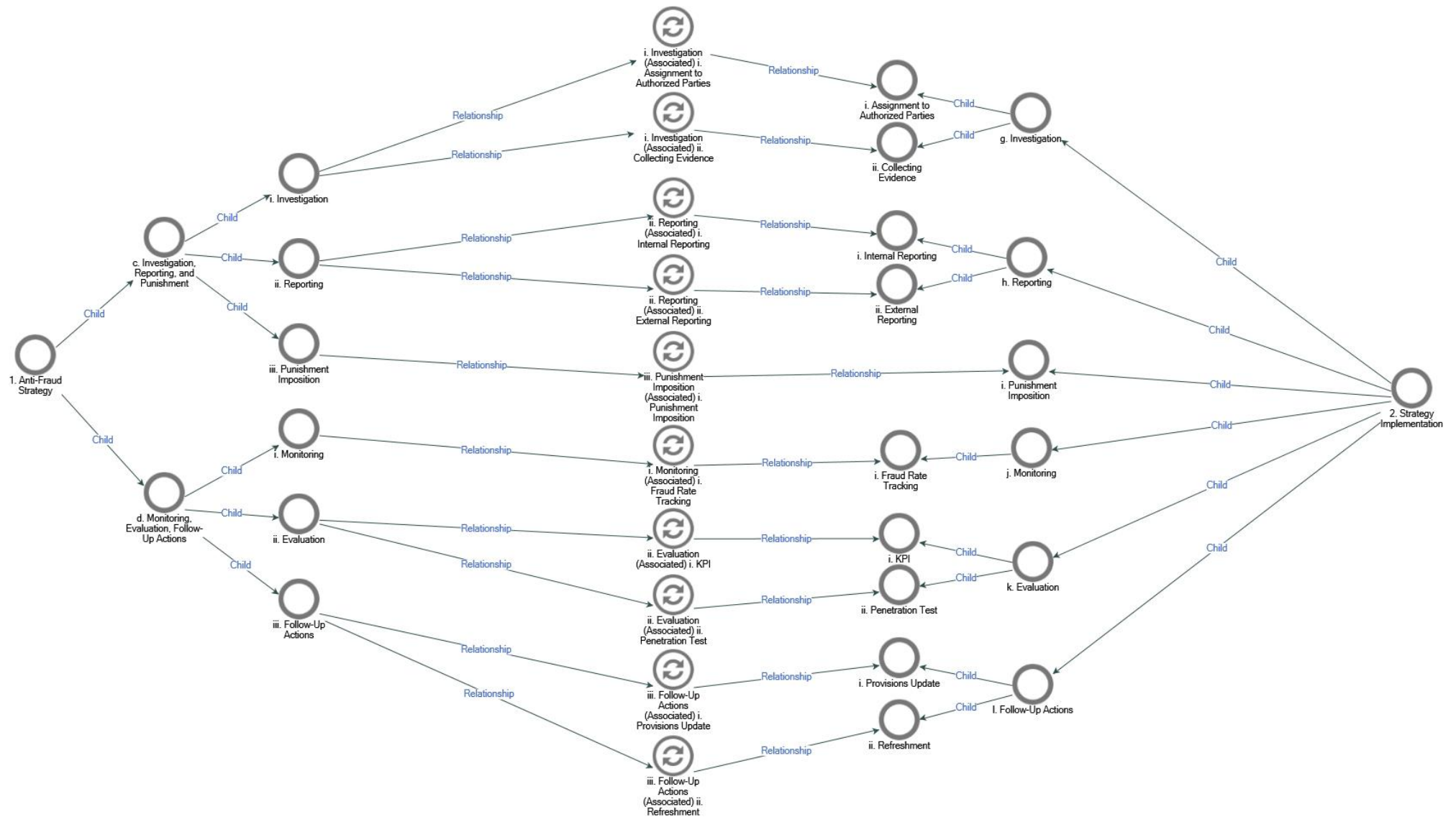


Figure 4.11 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Prevention



Source: Analyzed by The Researcher using NVivo 15

Figure 4.12 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Detection



Source: Analyzed by The Researcher using NVivo 15

Figure 4.13 Analytical Map of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman Focused on Investigation, Reporting, and Punishment and Monitoring, Evaluation, and Further Action

	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact
1. Anti-Fraud Strategy	No	No	No	No	No	No	No	No	No
a. Prevention	No	No	No	No	No	No	No	No	No
i. Anti-Fraud Awareness	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ii. Fraud Risk Identification	No	No	No	No	No	Yes	No	No	No
iii. Know Your Employee	No	No	No	No	No	No	No	No	No
b. Detection	No	No	No	No	No	No	No	No	No
i. Whistleblowing System	No	No	Yes	No	No	No	No	No	No
ii. Surprise Audit	No	No	No	No	No	No	No	No	No
iii. Surveillance System	No	No	No	No	No	No	No	No	Yes
c. Investigation, Reporting, and Punishment	No	No	No	No	No	No	No	No	No
i. Investigation	No	No	No	No	No	No	No	No	No
ii. Reporting	No	No	No	No	No	No	No	No	No
iii. Punishment Imposition	No	No	No	No	No	Yes	No	No	No
d. Monitoring, Evaluation, Follow-Up Actions	No	No	No	No	No	No	No	No	No
i. Monitoring	No	No	No	No	No	No	No	No	No
ii. Evaluation	No	No	No	No	No	No	No	No	No
iii. Follow-Up Actions	No	No	No	No	No	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System
1. Anti-Fraud Strategy	No	No	No	No	No	No	No	No	No
a. Prevention	No	No	No	No	No	No	No	No	No
i. Anti-Fraud Awareness	No	No	No	No	No	No	Yes	Yes	Yes
ii. Fraud Risk Identification	No	Yes	Yes	Yes	No	No	No	Yes	Yes
iii. Know Your Employee	No	No	No	No	No	Yes	Yes	Yes	No
b. Detection	No	No	No	No	No	No	No	No	No
i. Whistleblowing System	No	No	No	No	No	No	No	No	Yes
ii. Surprise Audit	No	No	No	No	No	No	No	No	No
iii. Surveillance System	No	No	No	No	No	No	No	No	No
c. Investigation, Reporting, and Punishment	No	No	No	No	No	No	No	No	No
i. Investigation	No	No	No	No	No	No	No	No	No
ii. Reporting	No	No	No	No	No	No	No	No	No
iii. Punishment Imposition	No	No	No	No	No	No	No	No	Yes
d. Monitoring, Evaluation, Follow-Up Actions	No	No	No	No	No	No	No	No	No
i. Monitoring	No	No	No	No	No	No	No	No	No
ii. Evaluation	No	No	No	No	No	No	No	No	No
iii. Follow-Up Actions	No	No	No	No	No	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

	e. Surprise Audit	i. Planning	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check	iii. Audit Trail
1. Anti-Fraud Strategy	No	No	No	No	No	No	No	No	No
a. Prevention	No	No	No	No	No	No	No	No	No
i. Anti-Fraud Awareness	No	No	No	No	No	No	No	No	No
ii. Fraud Risk Identification	No	No	Yes	No	No	No	Yes	Yes	Yes
iii. Know Your Employee	No	No	No	No	No	No	No	No	No
b. Detection	No	No	No	No	No	No	No	No	No
i. Whistleblowing System	No	No	No	No	No	No	No	No	No
ii. Surprise Audit	No	Yes	Yes	Yes	Yes	No	No	No	No
iii. Surveillance System	No	No	No	No	No	No	Yes	Yes	Yes
c. Investigation, Reporting, and Punishment	No	No	No	No	No	No	No	No	No
i. Investigation	No	No	No	No	No	No	No	No	No
ii. Reporting	No	No	No	No	No	No	No	No	No
iii. Punishment Imposition	No	No	No	No	No	No	No	No	No
d. Monitoring, Evaluation, Follow-Up Actions	No	No	No	No	No	No	No	No	No
i. Monitoring	No	No	No	No	No	No	No	No	No
ii. Evaluation	No	No	No	No	No	No	No	No	No
iii. Follow-Up Actions	No	No	No	No	No	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
1. Anti-Fraud Strategy	No	No	No	No	No	No	No	No	No
a. Prevention	No	No	No	No	No	No	No	No	No
i. Anti-Fraud Awareness	No	No	No	No	No	No	No	No	No
ii. Fraud Risk Identification	No	Yes	Yes	Yes	No	No	No	No	No
iii. Know Your Employee	No	No	No	No	No	No	No	No	No
b. Detection	No	No	No	No	No	No	No	No	No
i. Whistleblowing System	No	No	No	Yes	No	Yes	No	No	No
ii. Surprise Audit	No	No	No	No	No	No	No	No	No
iii. Surveillance System	Yes	Yes	Yes	No	No	No	No	No	No
c. Investigation, Reporting, and Punishment	No	No	No	No	No	No	No	No	No
i. Investigation	No	No	No	No	Yes	Yes	No	No	No
ii. Reporting	No	No	No	No	No	No	No	Yes	Yes
iii. Punishment Imposition	No	No	No	No	No	No	No	No	No
d. Monitoring, Evaluation, Follow-Up Actions	No	No	No	No	No	No	No	No	No
i. Monitoring	No	No	No	No	No	No	No	No	No
ii. Evaluation	No	No	No	No	No	No	No	No	No
iii. Follow-Up Actions	No	No	No	No	No	No	No	No	No

Source: Analyzed by The Researcher using NVivo 15

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test	I. Follow-Up Actions	i. Provisions Update	ii. Refreshment
1. Anti-Fraud Strategy	No	No	No	No	No	No	No	No	No
a. Prevention	No	No	No	No	No	No	No	No	No
i. Anti-Fraud Awareness	No	No	No	No	No	No	No	No	No
ii. Fraud Risk Identification	No	No	No	No	No	No	No	No	No
iii. Know Your Employee	No	No	No	No	No	No	No	No	No
b. Detection	No	No	No	No	No	No	No	No	No
i. Whistleblowing System	No	No	No	No	No	No	No	No	No
ii. Surprise Audit	No	No	No	No	No	No	Yes	No	No
iii. Surveillance System	No	No	No	No	No	No	No	No	No
c. Investigation, Reporting, and Punishment	No	No	No	No	No	No	No	No	No
i. Investigation	Yes	No	No	No	No	No	Yes	No	No
ii. Reporting	No	No	No	No	No	No	Yes	No	No
iii. Punishment Imposition	Yes	Yes	No	No	No	No	No	No	No
d. Monitoring, Evaluation, Follow-Up Actions	No	No	No	No	No	No	No	No	No
i. Monitoring	No	No	Yes	No	No	No	No	No	No
ii. Evaluation	No	No	No	No	Yes	Yes	No	No	No
iii. Follow-Up Actions	No	No	No	No	No	No	No	Yes	Yes

Source: Analyzed by The Researcher using NVivo 15

Figure 4.14 Matrix Coding of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

4.3.1 Prevention

Prevention constitutes the first pillar in the implementation of the anti-fraud strategy at PT BPR Bank Sleman and is intended to reduce the possibility of fraud before it occurs. Referring to PT BPR Bank Sleman (2024), this pillar is designed as a structured set of controls meant to address fraud risk at an early stage, before it develops into actual misconduct. Within this framework, prevention is carried out through three main programs, including anti-fraud awareness, fraud risk identification, and know your employee.

4.3.1.1 Anti-Fraud Awareness

The development of anti-fraud awareness at PT BPR Bank Sleman constitutes a central component of the Bank's fraud prevention efforts across the organizational level. This awareness is maintained not only through official guidelines but also through management's commitment to translating anti-fraud principles into concrete practices. Hence, in order to raise anti-fraud awareness, PT BPR Bank Sleman undertakes the following efforts:

1. Anti-Fraud Team

Team formation serves as the first step towards anti-fraud awareness. PT BPR Bank Sleman formed a cross-functional Anti-Fraud Strategy Implementation Team (*Tim Penerapan Strategi Anti Fraud atau TIM SAF*) to support the implementation of anti-fraud measures across the

organization. According to Miharjo (2025), the qualification of this team is determined by each unit's applicability and proficiency in handling fraud-related issues, specifically, Internal Audit, Risk Management, Human Capital, and Compliance. This explanation supports Setiawan (2025), who claims Internal Audit collaborates with Compliance and Risk Management within the SAF Team, indicating that anti-fraud efforts are dispersed throughout several departments rather than concentrated in one department. Within this structure, each unit has a distinct function. Referring to Miharjo (2025), Human Capital is in charge of managing whistleblowing systems and issues pertaining to punishment. In contrast, Risk Management is primarily responsible for preventing fraud before it occurs through socialization, education, and awareness-building. In this regard, Dewi (2025) added that anti-fraud socialization is carried out jointly by the SAF Team, while the Compliance function typically provides policy-related documents. Setiawan (2025), as the Senior Internal Audit Staff, on the other hand, pointed out that Internal Audit typically becomes more involved after an indication has emerged, emphasizing its role in the subsequent handling of anti-fraud cases. Referred to Director's Decree Number

107/KPTS/DIR/2024, this team has been formally arranged and has direct accountability to the Director of Compliance (PT BPR Bank Sleman, 2024).

2. Anti-Fraud Training

Anti-fraud training is implemented as a regular learning mechanism designed to ensure that employees comprehend anti-fraud concepts, relevant procedures, and emerging fraud risks. Anti-fraud training is mandatory for all employees at least once a year, in addition to other programs such as APU-PPT and customer protection training (Setiawan, 2025). Dewi (2025) emphasized that fraud-related training is held annually because all employees are expected to understand fraud and compliance issues. This recurring approach is further supported by regular anti-fraud socialization conducted by the SAF Team (Chitra, 2025).

Beyond the mandatory annual training for all employees, anti-fraud training is also extended in accordance with the needs of specific units. Setiawan (2025) noted that Internal Audit staff are given further training whenever new audit-related issues or regulatory changes arise, either through internal programs organized by the Bank or through external providers. In terms of delivery, anti-fraud training itself may involve speakers from

individual practitioners or private institutions (Chitra, 2025). The material covered goes beyond traditional fraud like financial loss, as Miharjo (2025) indicated that training in Risk Management includes topics such as digital fraud, data leakage, confidentiality breaches, and related areas of fraud, audit, compliance, and APU-PPT to strengthen employee competence.

A structured planning and evaluation process is applied as part of anti-fraud training enforcement. The annual training plan is formulated based on risk considerations, performance evaluation, and proposals from each unit. Its effectiveness is then assessed through pre-tests and post-tests attached to each training activity to measure participants' seriousness and understanding (Chitra, 2025). Miharjo (2025) remarked that the training had been effective, as it enabled employees to gain a new understanding and grasp of tools that could later support their work practices.

3. Competence Certification

In supporting anti-fraud strategy implementation, competence development is carried out through certification, specifically in the Internal Audit unit, in addition to participation in technical training. Setiawan

(2025) noted that Internal Audit personnel had attended various forms of professional development, such as investigative audit and IT audit. This was reflected in the following statement:

“Sejauh ini sangat membantu, jadi kita pun Alhamdulillah untuk tim SKAI Bank Sleman, itu kita tiga orang, jadi ada kepala SKAI, kemudian staff-nya dua. Itu kebanyakan sudah kita ikutkan untuk sertifikasi juga, sertifikasi khusus untuk PE, jadi Pejabat Eksekutif Audit Internal. Istilahnya kita sudah ada kompetensi juga.” (Setiawan, 2025)

4. Regulations and Provisions Formulation

The formulation of anti-fraud provisions at PT BPR Bank Sleman is supported by formal instruments that have already been established within the Bank. Chitra (2025) and Setiawan (2025) indicated that the anti-fraud mechanism has been equipped with the necessary instruments, including SOPs and provisions that must be followed across the work unit. In practice, Dewi (2025), as the Legal Compliance, and APU-PPT Department Staff, explained that the Compliance department ensures that anti-fraud policies are first aligned with POJK and SEOJK requirements, and that the implementation is then supported through socialization to foster employees' understanding of the relevant provisions.

The process, however, does not stop at formulation. Dewi (2025) further noticed that the adequacy of existing

provisions is continuously assessed through indicators such as the presence or absence of fraud cases and the post-test results following dissemination activities. The current regulations are examined, and may be refreshed, revised, or supplemented with new provisions, when repeated findings appear in specific areas or when certain units are determined to lack sufficient provisions. This review is carried out in coordination with Internal Audit, as audit findings may reveal recurrent infractions, non-compliance, or control gaps that require regulatory adjustment. In the same vein, Miharjo (2025) outlined that the Compliance department also examines whether fraud cases stem from flaws in existing regulations, indicating that internal rules are regularly evaluated as part of the Bank's preventive efforts.

5. Anti-Fraud Publication

Anti-fraud publication at PT BPR Bank Sleman serves as part of the Bank's effort to promote awareness and vigilance against fraud among customers and other external parties (PT BPR Bank Sleman, 2024). Practically, this publication is embedded in the Bank's working environment through routine visual reminders, including anti-fraud messages displayed, such as "zero fraud" on office

televisions (Setiawan, 2025). This was further illustrated by

Dewi (2025):

“Kemudian juga di desktop-nya PC karyawan masing-masing, itu sudah kita tampilkan wallpaper-nya itu adalah anti fraud, misalkan jangan lakukan fraud, terus keluarga di rumah menunggu, kayak gitu. Kemudian kita juga di depan itu kan ada TV, di semua kantor cabang juga ada TV, di depan akses itu juga ada, kita buat dan tampilkan poster anti fraud.” (Dewi, 2025)

Additionally, Chitra (2025) described publication efforts through poster installation as a reminder about the danger of fraud, as well as reading the banker’s code of ethics during morning briefings.

6. Anti-Fraud Socialization

Beyond the awareness conveyed through anti-fraud publication to external parties, anti-fraud awareness at PT BPR Bank Sleman is strengthened internally through anti-fraud socialization conducted routinely at the unit level and accompanied by refreshment sessions delivered by the Anti-Fraud Team (Setiawan, 2025). Miharjo (2025) explained that socialization is conducted through monthly visits to different departments because it is considered more effective than gathering all employees in one place. These visits educate employees about preventing fraud and encourage them to identify it more broadly, not just as direct theft but also as actions like data leaks and conflicts of

interest that should be recognized early on in all work units. This approach is reinforced by the Bank's monthly rotating socialization for all employees and implemented across divisions as part of a broader effort to cultivate an anti-fraud culture (Chitra, 2025; Dewi, 2025). As Miharjo (2026) stated:

“Saya rasa pemahaman anti fraud itu seluruhnya wajib dipahami oleh insan perbankan dari golongan apapun. Dan itu yang kita lakukan. Kita melakukan sosialisasi anti-fraud itu bukan cuman hanya ke bawah, bahkan sampai level tertentu, misalnya OB tadi dan lain-lain itu juga kita sampaikan juga bahwa terkait dengan pentingnya pemahaman anti fraud.”

7. Integrity Pact

The final implementation layer is the signing of the integrity pact as part of the Bank's effort to build an anti-fraud culture (Chitra, 2025). This practice functions as a formal and recurring reaffirmation of employees' commitment to anti-fraud values and is carried out alongside the signing of the banking code of ethics and anti-fraud declarations as part of the Bank's preventive efforts (Miharjo, 2025). Although the reported timing differs slightly, with one referring to annual implementation and another to a six-month cycle, both indicate that the integrity pact is treated as an ongoing commitment rather than a one-time formality (Chitra, 2025; Miharjo, 2026).

4.3.1.2 Fraud Risk Identification

Fraud risk identification constitutes the second preventive component in the implementation of the anti-fraud strategy at PT BPR Bank Sleman. This component aims to identify vulnerabilities and recognize potential fraud risks inherent in activities that potentially cause losses to the Bank, with the results being documented, communicated to relevant parties, and regularly updated, particularly for high-risk activities (PT BPR Bank Sleman, 2024). Thus, fraud risk identification at PT BPR Bank Sleman is carried out through the following efforts:

1. Fraud Detection System

Fraud Detection System is one of the tools used in fraud risk identification at PT BPR Bank Sleman, especially in digital banking transactions. According to Dewi (2025), the Fraud Detection System (FDS) is integrated into the program and uses preset parameters to detect questionable activity in ATM and virtual account transactions. The system may immediately restrict an account when a transaction meets the red-flag criteria. Verification follows to ascertain if the transaction was genuinely conducted by the customer or by an unauthorized party. In more specific terms, Miharjo (2025), as Risk Management Staff, stated:

“FDS itu Fraud Detection System. Jadi Fraud Detection System ini berfungsi untuk menganalisa atau menetapkan

hal-hal yang di luar batas normal. Jadi itu parameterized ya, jadi itu ada parameternya. Parameternya itu misalnya seperti, oh ada transaksi ATM dilakukan secara bersamaan di selang waktu bersamaan, gitu. Jadi, itu FDS kita ngebaca itu, sistem kita ngebaca itu. Atau misalnya ada bukan nasabah tapi berhasil melakukan transaksi seperti itu. Atau ada rekening pasif tapi dapat melakukan transaksi. Jadi hal-hal yang tidak normal itu akan diketahui oleh FDS namanya, Fraud Detection System.”

As a further step, cases that are confirmed as fraud are escalated to Internal Audit, whereas unproven indicators are addressed at the Risk Management level (Miharjo, 2025). These indicate that the FDS serves as an early detection system for spotting anomalous transactions before they are examined further.

2. Risk Register

Fraud risk identification is also enforced through periodic risk documentation in the form of a risk register. Miharjo (2025) pointed out that the risk register is updated every month by work units across the Bank, albeit certain units may occasionally be late. This demonstrates how fraud risk is tracked through a continuous procedure where each unit is expected to regularly identify and document its risk exposure, as opposed to merely reacting after a fraud occurrence has taken place.

3. Profile Risk Scoring

Profile risk scoring comprises another mechanism through which fraud risk is assessed at PT BPR Bank Sleman. This process is carried out within a regulatory framework rather than based on arbitrary internal judgment, as it refers to OJK Circular Letter Number 1/SEOJK.03/2019 on the Implementation of Risk Management for Rural Banks. Accordingly, the assessment of fraud-related risk exposure is conducted in a structured and standardized manner in line with the applicable regulatory provisions (Miharjo, 2025).

4.3.1.3 Know Your Employee

Know Your Employee (KYE) at PT BPR Bank Sleman represents a human resource control within the Bank's fraud prevention efforts. Rather than being limited to employee identification at the entry point, KYE is applied as a recurring control to reduce the fraud risk (PT BPR Bank Sleman, 2024). This is reflected in several measures related to employee management and supervision at PT BPR Bank Sleman.

1. Employee Recruitment

Employee recruitment represents the initial control stage in the KYE implementation at PT BPR Bank Sleman. This stage is intended to provide a complete and accurate picture

of each candidate's background and to ensure that recruitment is conducted through appropriate, objective, and transparent qualifications (PT BPR Bank Sleman, 2024). Chitra (2025), as Human Capital department staff, expressed that the recruitment process is performed under a written SOP and begins with document screening, followed by user interviews, psychological or basic competency test, medical check-ups, and interviews with directors. The process also considers competencies such as analytical thinking, communication skills, and legal understanding (Chitra, 2025). Background checks are also incorporated into the recruitment process, as illustrated in the following statement:

“Rekam jejak pegawai dilakukan untuk semua calon pegawai. Apabila calon pegawai sudah pernah bekerja, maka dilakukan pengecekan ke perusahaan lama, cross check dengan bagian HRD apakah calon pegawai tersebut memiliki rekam jejak yang baik atau kurang baik di perusahaan sebelumnya. Selain itu saat ini sudah ada aplikasi SIPELAKU dari OJK sehingga bagian SDM bisa mengecek apakah calon pegawai tersebut pernah terlibat dalam tindakan fraud sebelumnya. Tujuannya untuk menghindari penerimaan pegawai yang memiliki rekam jejak yang kurang baik.” (Chitra, 2025)

2. Internal Employee

The implementation of Know Your Employee at PT BPR Bank Sleman goes beyond recruitment and continues through the monitoring of internal employees. This stage

focuses on recognizing and observing employees' character, behavior, and lifestyle (PT BPR Bank Sleman, 2024). This is enacted through periodic background checks, involving regular SLIK BI reviews, monitoring of employees' social media, and observation of employees' lifestyle at work or, in certain cases, through visits to their residences. Among these measures, SLIK checking was considered the most effective as it may reveal financial conditions that could indicate vulnerability, such as risky online loans or pay-later obligations (Chitra, 2025).

3. Employee Turnover

Another aspect of Know Your Employee at PT BPR Bank Sleman relates to how employee rotation and turnover are managed. PT BPR Bank Sleman (2024) stated that promotion, mutation, and staff placement are expected to be conducted objectively and transparently while taking risk considerations into account, particularly for positions with higher fraud exposure. Setiawan (2025) indicated that rotation is carried out according to organizational needs and may therefore take quite a long time in certain cases. Similarly, it is noted that rotation is not executed too frequently and is generally undertaken every three to five years, since certain functions, specifically Risk

Management, require personnel with integrity, sound banking knowledge, and strong judgment (Chitra, 2025; Miharjo, 2025). This relatively limited level of employee movement was also reflected in the following statement:

“Turnover cukup rendah ya, rata-rata satu sampai dua pegawai per tahun, dengan jumlah pegawai 170 orang.”
(Chitra, 2025)

4.3.2 Detection

The second pillar in PT BPR Bank Sleman’s anti-fraud strategy is detection, which focuses on identifying possible fraud as soon as irregularities develop. This pillar aims to capture indications that require further scrutiny. Referring to PT BPR Bank Sleman (2024), the detection pillar is implemented through formal reporting, examination, and monitoring mechanisms. Consequently, three primary programs are discussed as detection pillars in this study.

4.3.2.1 Whistleblowing System

Whistleblowing system (WBS) is positioned as a mechanism for handling fraud complaints, supported by a separate reporting and follow-up procedure as well as protection for the reporter’s identity (PT BPR Bank Sleman, 2024). Reports may be submitted by both internal and external parties. External parties may report alleged misconduct involving Bank employees through the Bank Sleman website, while internal parties may submit reports either through the website or directly to the designated

whistleblowing officer in the HR unit (Dewi, 2025). The dissemination of the WBS is also supported by a dedicated guideline that has been shared through the internal policy portal, so that employees can access it freely. It is further introduced during socialization in each work unit by the Anti-Fraud Team, including the monthly visits conducted across departments as part of anti-fraud awareness activities (Chitra, 2025; Miharjo, 2025). Once a report is received, the whistleblowing officer first reviews whether sufficient initial evidence is available before forwarding the case to the appropriate parties for further handling, including the Internal Audit department if needed (Dewi, 2025; Miharjo, 2025).

Protection of the reporter is treated as an essential part of the system. As indicated by Dewi (2025), this protection includes confidentiality of the whistleblower's identity, the provision of legal assistance where the case proceeds to court, and the possibility to make remarks without direct confrontation with the reported party during the investigation process. It also covers protection against reprisal, from blacklisting, intimidation, termination, or legal action, and protection against external threats, depending on the type of threat the whistleblower reported.

4.3.2.2 Surprise Audit

PT BPR Bank Sleman (2024) indicates that a surprise audit is a sudden and unannounced examination intended to maintain

employee alertness and ensure that duties are performed in accordance with established procedures. The implementation of a surprise audit at PT BPR Bank Sleman is reflected in four aspects:

1. Planning

The planning of the surprise audit is arranged on a risk basis. Setiawan (2025) defined that the planning stage is prepared by considering fraud risk and vulnerabilities that may give rise to misuse or irregularities. At this stage, the scope, object, and focus of the examination are first determined before the audit is performed. This is accompanied by an annual audit plan for work units, while a surprise audit may also be undertaken when an indication of fraud arises (Dewi, 2025; Setiawan, 2025).

2. Inspection

Inspection embodied the execution stage of a surprise audit, following planning and preceding the reporting and follow-up stages. During this phase, the audit is conducted directly by Internal Audit by examining work units on the spot (Dewi, 2025). Setiawan (2025) stated that the inspection aims to assess whether SOPs have been properly applied, spot anomalous trends or non-compliance, and evaluate vulnerabilities discovered during the audit process.

3. Cash Opname

A routine part of a surprise audit at PT BPR Bank Sleman is cash opname. As reflected in Setiawan (2025), Senior Internal Audit Staff:

“Kalau yang penting kita setiap bulan pasti minimal ada satu kali kas opname ya, jadi terutama untuk kas besar, di brankas itu ya kita berusaha untuk itu, surprise audit kita cek, kemudian juga kaitannya inventaris seperti tabungan, materai, dan lain-lain itu juga kita cek, minimal itu sih.”

This indicates that cash opname is conducted at least once every month and is focused on cash in the vault, as well as related inventories under internal control. The timing is arranged randomly to maintain the surprise element as the audit involves cash and other material values that require stricter monitoring. This routine is performed across all units, both in the head office and branch offices. It is conducted without specific indicators to determine the object of examination, as it serves as an initial safeguarding measure, considering that cash is the Bank's primary asset (Setiawan, 2025). This reflects that cash opname operates as a detection mechanism while maintaining the element of surprise, particularly in reducing opportunities for anomalies in cash handling.

4. External Audit

A surprise audit may also be conducted by external auditors. PT BPR Bank Sleman (2024) stated that such audits can be executed by either internal or external parties without prior notification. Referring to Setiawan (2025), PT BPR Bank Sleman is subject to external audits, mainly related to IT inspections, which are conducted periodically, generally once every three years. These audits also extend to internal audit evaluation in assessing the extent to which audit activities have been carried out within the Bank. This indicates that external audit represents an additional layer of oversight, complementing internal audit while ensuring the audit functions align with established standards.

4.3.2.3 Surveillance System

The third program under the detection pillar is the surveillance system. PT BPR Bank Sleman (2024) defined a surveillance system as a form of confidential testing or examination conducted without the knowledge of the party being observed in order to monitor and test the effectiveness of anti-fraud policies. Based on the findings, the implementation of this program can be seen in six aspects:

1. CCTV

The use of CCTV across the Bank's premises serves as one of the forms of an implemented surveillance system at PT BPR Bank Sleman. Miharjo (2026) specified that all corners of the rooms have been equipped with CCTV, which is particularly useful in tracing discrepancies involving physical cash, especially in teller activities. It works as authentic evidence to review processes or specific events that may lead to shortages, differences, or other irregularities.

2. Red Flag Check

The surveillance system is also deployed through red flag checking embedded in the Bank's system. As per Miharjo (2025) the Bank's core banking system has contained parameters and red flags to identify suspicious transactions or unusual activities. This is supported by the use of the Fraud Detection System (FDS) in digital transactions, where unusual patterns are detected automatically and then followed up for further investigation (Dewi, 2025). From the audit side, transaction logs and irregular patterns are also reviewed as part of IT-based monitoring (Setiawan, 2025).

3. Audit Trail

Miharjo (2025) indicated that an audit trail has been implemented at PT BPR Bank Sleman to trace suspicious transactions and system access, as reflected in the following statement:

“Kemudian yang kedua, sistem juga itu bisa punya audit trail. Jadi audit trail itu bagaimana sistem ini akan mengetahui siapa saja yang mengakses sistem tersebut, jam berapa bisa mengakses, dan apa yang diakses, aa yang di-download. Jadi semua backend dari sistem tersebut terbaca oleh audit trail. Nah, itu hal-hal yang tidak diketahui oleh petugas, karena petugas tidak punya akses tersebut.” (Miharjo, 2026)

Audit trail is also required to record user access, the action performed, and any changes made in the system, as well as transaction activities reviewed through log user checks (Dewi, 2025; Setiawan, 2025).

4. Job Desk Check

According to Setiawan (2025), the implementation of work procedures is evaluated based on the applicable SOPs and job descriptions in each unit. When duties are enacted in ways that are not in accordance with these provisions, such conditions may lead to fraud opportunities. The application of rolling sessions supports this and leaves substitution, specifically for tellers, where the work of one employee can be reviewed by another. The risk of collusion or irregularities could be reduced (Miharjo, 2026).

5. Attached Supervision

The implementation of attached supervision is described in the following statement:

“Kemudian juga pengawasan melekat, baik itu secara offline yang misalnya target paraf, tanda tangan, dan lain-lain, itu semua ter-record. Jadi, pengawasan melekatnya itu terinventarisir dengan baik. Nah, itu yang membuat, seharusnya membuat orang-orang ketika melakukan fraud itu sulit untuk melakukan. Jadi, kita membuat sistem struktur organisasi yang flow-nya itu lengkap untuk meminimalisir potensi-potensi teman-teman melakukan kecurangan.” (Miharjo, 2025)

This is also supported by supervisor confirmation, approval mechanisms, and work reviews, which are emphasized on functions vulnerable to fraud (Dewi, 2025; Miharjo, 2026). Additionally, in line with the KYE implementation for internal employees, periodic SLIK BI checks, social media and lifestyle monitoring, as well as background checks through SIPELAKU, serve as forms of attached supervision (Chitra, 2025).

6. Authorization

Authorization is also one of the surveillance systems implemented at PT BPR Bank Sleman. Referred to Miharjo (2025), access to the system is not granted to all employees, as only authorized personnel are allowed to enter certain parts of the system. In line with that, system access requires a user ID and password, which allows the access and

activities of each user to be identified (Dewi, 2025). Besides, Miharjo (2026) pointed out that authorization is conducted in stages and does not rely on a single authorization, as dual control or double check is also applied in the process.

4.3.3 Investigation, Reporting, and Punishment

The third pillar in PT BPR Bank Sleman's anti-fraud strategy is response, which focuses on handling fraud indications that have been detected and required further treatment. This pillar aims to ensure that each indication of fraud is processed through proper investigation, reporting, and punishment imposition for the fraud perpetrators (PT BPR Bank Sleman, 2024).

4.3.3.1 Investigation

Investigation is conducted to follow up indications of fraud and to collect evidence related to suspected misconduct. PT BPR Bank Sleman (2024) specified that investigation forms as an important part of the fraud control system, as every detected indication of fraud should be processed in accordance with investigation standards while maintaining the confidentiality of the information obtained. In practice, investigation is executed by Internal Audit to perform a deeper analysis of indications supported by sufficient initial evidence (Dewi, 2025; Miharjo, 2025). Setiawan (2025), as Senior Internal Audit Staff, explained that

Internal Audit may investigate after the President Director issues a formal assignment. Regarding independence, Setiawan (2025) further stated that:

“Untuk menjaga independensi kan kita tidak boleh terlibat di operasional langsung, jadi kebetulan kalau di bagian lain, dulu saya masih di analis itu bisa jadi tim pengadaan dan sebagainya, tapi kalau kita sudah di Audit Internal, kita tidak bisa terlibat, untuk menjaga independensi. Kalaupun mau memeriksa pun, misalnya saya dari bagian analis, saya mau memeriksa bagian yang saya sebelumnya, kita juga sesuai ketentuannya, di OJK pun harus ada minimalnya berapa bulan baru bisa masuk periksa.”

The investigation process is then followed by evidence collection to support further analysis. Setiawan (2025) indicated that once the assignment has been issued, the investigation is planned by determining the roles, inputs, and timeline, after which evidence is collected and analyzed. The evidence may be obtained from documents, on the spot examination, direct interviews, and transaction tracing such as vouching. The findings are then used to formulate a brief statement of facts, chronology, and possible losses.

4.3.3.2 Reporting

Reporting is conducted to communicate the fraud cases and how they've been handled to both internal and external related parties. According to PT BPR Bank Sleman (2024), reporting in the implementation of anti-fraud strategy includes periodic reporting as well as the reporting of significant fraud incidents to OJK within the required timeframe. Within this regard, internal reporting is

carried out after the investigation process has been completed. Miharjo (2026) stated that reporting is prepared in accordance with the case development and the extent to which the indication has been substantiated. Setiawan (2025) described that the findings are reported to the President Director, followed by reporting to the Board of Commissioners through the Audit Committee, with copies forwarded to related internal parties, including the compliance department. Additionally, the report may include recommendations for further action based on the results obtained.

Moreover, external reporting is conducted as part of the Bank's regulatory obligation. PT BPR Bank Sleman (2024) indicated that the anti-fraud strategy implementation is reported to OJK on a semester basis, while significant fraud incidents must be reported no later than three working days after they are identified. Following this, Miharjo (2025) stated that all fraud incidents remain subject to routine reporting to OJK, including nil reporting when no fraud occurs. Setiawan (2025) also pointed out that fraud investigation reports may be forwarded to OJK as part of the formal reporting flow.

4.3.3.3 Punishment Imposition

PT BPR Bank Sleman (2024) explained that the Bank implements sanctions that are effective, fair, transparent, consistent, and capable of creating a deterrent effect, in accordance with

company regulations and applicable laws. This process is handled by the Human Capital department, which determines whether the case constituted fraud and what sanctions should be imposed, with the recommendations provided by Internal Audit (Dewi, 2025; Miharjo, 2025; Setiawan, 2025). The punishment imposed may include disciplinary measures, demotion, or dismissal for employees proven to have engaged in fraud or other misconduct (Chitra, 2025).

4.3.4 Monitoring, Evaluation, and Further Action

The fourth pillar in PT BPR Bank Sleman's anti-fraud strategy is monitoring, evaluation, and follow-up action, which focuses on assessing the implementation of anti-fraud measures and identifying areas that require improvement. This aimed to ensure that fraud handling and control measures are continuously reviewed so that similar weaknesses do not recur (PT BPR Bank Sleman, 2024).

4.3.4.1 Monitoring

Monitoring is performed to oversee the follow-up of findings related to fraud and to track the fraud occurrence within the Bank. PT BPR Bank Sleman (2024) described that monitoring focuses on the follow-up of fraud reports in accordance with the Bank's internal provisions and applicable regulations. Setiawan (2025) explained that after deviations or non-compliance are identified, recommendations and follow-up actions are given and

later reviewed again to assess the extent to which they have been implemented. Monitoring is also conducted by observing whether fraud occurs within a certain year and by reviewing findings identified by Internal Audit as part of the implementation of anti-fraud measures (Dewi, 2025).

4.3.4.2 Evaluation

PT BPR Bank Sleman (2024) stated that fraud incident data are maintained as an evaluation tool, covering information such as perpetrators, positions, follow-up status, fraud type, related activities, modus operandi, location, affected division, injured party, time of occurrence, amount of loss, fraud causes, handling actions, and corrective actions for fraud prevention. Based on these data, weaknesses and fraud causes may be traced and used to determine the necessary corrective measures, while the overall evaluation of the fraud control system is conducted periodically. One form of evaluation implemented at PT BPR Bank Sleman is reflected through the use of Key Performance Indicators (KPI). Miharjo (2025) described that anti-fraud implementation is not assessed through a specific KPI assigned to the Anti-Fraud Team, but rather through individual KPI in each related unit, and employees involved in fraud may also experience a decline in their KPI. In a similar vein, Chitra (2025) specified that employee

performance evaluation is conducted every semester through this system.

Furthermore, evaluation is also performed through annual penetration tests and the review of fraud-related findings. Dewi (2025) explained that penetration tests are conducted every year, while also being undertaken by reviewing whether fraud occurred within the year, examining internal audit findings related to fraud, and identifying weaknesses in internal provisions that may have contributed to such incidents. Besides, the effectiveness of anti-fraud socialization and training may be seen from pre-test and post-test results, and from whether fraud occurs within the year (Chitra, 2025; Dewi, 2025).

4.3.4.3 Further Actions

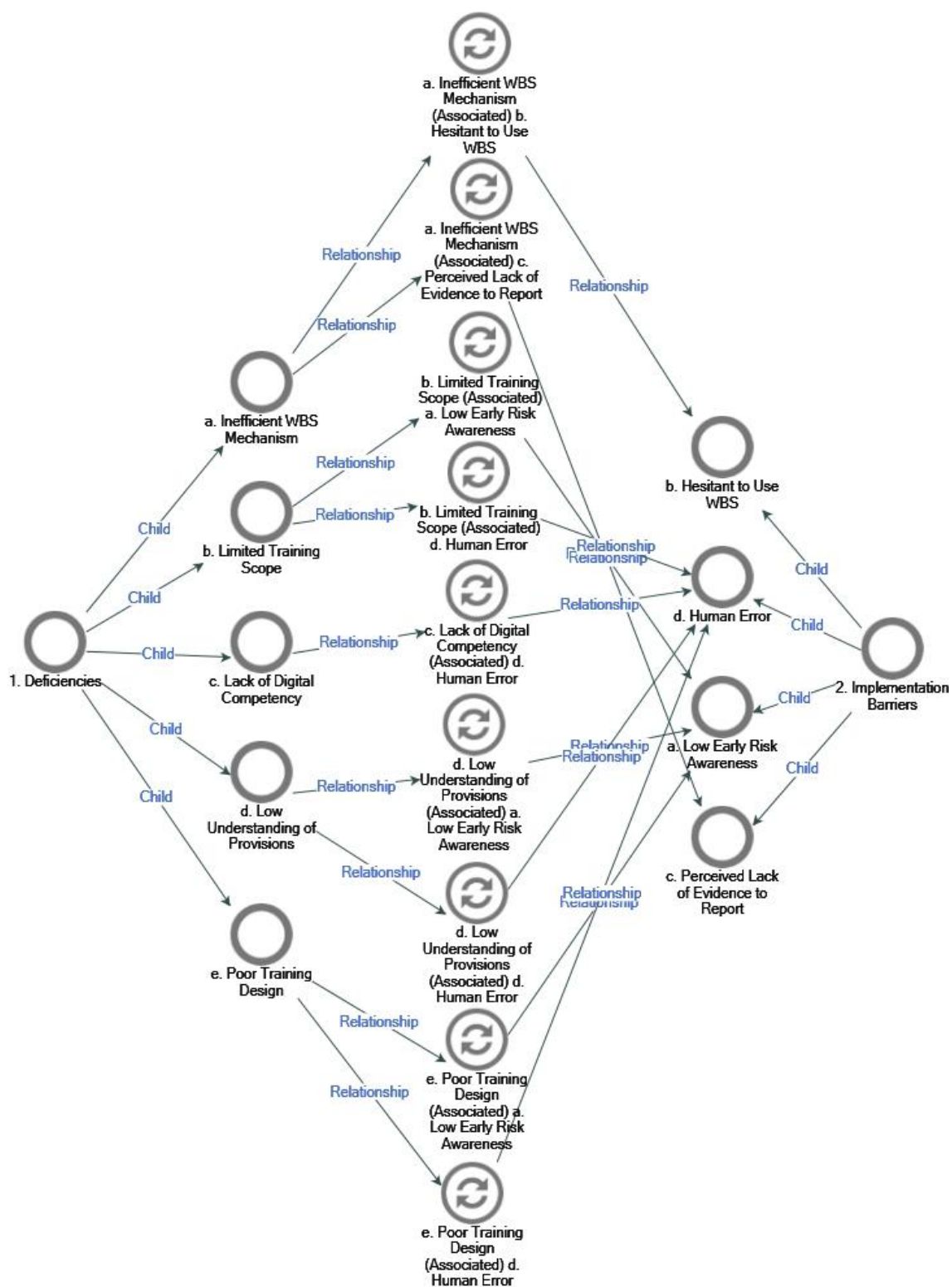
Follow-up actions are conducted to address weaknesses identified through the evaluation of fraud incidents and to strengthen internal control so that similar fraud does not recur. PT BPR Bank Sleman (2024) indicated that it is arranged based on the evaluation's results in order to improve weaknesses and reinforce the internal control system. Update for internal provisions is one kind of follow-up action. Dewi (2025) explained that when findings indicate that existing policies are no longer adequate or that certain risky conditions have not yet been regulated, the relevant provisions are reviewed, refreshed, or revised in coordination with Internal

Audit. Chitra (2025) likewise stated that, based on the findings, the Anti-Fraud Team discusses the findings with management and may propose changes, updates, or formulate new regulations when needed.

Another kind of follow-up action at PT BPR Bank Sleman is refreshment. Dewi (2025) specified that refreshment is provided when repeated violations or similar questions indicate that employees may need a renewed understanding of certain provisions. This may take the form of repeated socialization or further explanation of the applicable rules by using real-life examples. Consistent with this, Chitra (2025) noted that the need for training may also be proposed based on fraud findings and management evaluations. This shows that follow-up actions at PT BPR Bank Sleman comprise reinforcement of employees' understanding, hence no recurrence of similar weaknesses.

4.4 Challenges Faced by PT BPR Bank Sleman in Anti-Fraud Strategy Implementation

This section discusses the challenges faced by PT BPR Bank Sleman in implementing anti-fraud strategies to minimize the occurrence of occupational fraud. Based on the NVivo analysis, the challenges could be grouped into two main categories, deficiencies and implementation barriers. The results of this analysis are presented in the figure below.



Source: Analyzed by The Researcher using NVivo 15

Figure 4.15 Analytical Map of Challenges Faced by PT BPR Bank Sleman in Implementing Anti-Fraud Strategies

4.4.1 Deficiencies

Deficiencies refer to weaknesses identified in the design or support of anti-fraud implementation. Based on the findings, several deficiencies were identified, including:

1. Inefficient WBS Mechanism

Although PT BPR Bank Sleman has already used a website-based whistleblowing system, the mechanism is still considered inefficient. Dewi (2025) illustrates it in the following statement:

“Kendalanya itu adalah ketika ada pelapornya, tapi tidak terdapat buktinya. Jadi SDM harus mencari dulu, ini apakah memang betul atau tidak. Nah, kemudian kalau memang tidak ada buktinya, kemudian itu cuma kayak gosip atau apa, itu kan tidak bisa ditindaklanjuti. Tapi dari kendala yang di web itu, itu memang juga belum sempurna ya, karena harusnya kan dia bukan satu form yang harus di-download, kemudian di-scan, habis itu di-upload, itu kan agak menyulitkan sebenarnya untuk whistleblower ya.”

This indicates that the inefficiency of the WBS is reflected both on the limited supporting evidence in some reports and in the reporting mechanism itself, which requires several manual steps before a report can be submitted.

2. Limited Training Scope

The findings also identify that the scope of anti-fraud training at PT BPR Bank Sleman remains limited. Despite anti-fraud strategy socialization has been conducted for all employees, training that focuses on specific fraud types and other supporting skills has not yet been provided more broadly across employees. Given this, Chitra (2025) stated:

“Untuk saat ini belum ada pelatihan, yang diwajibkan saat ini adalah pelatihan strategi anti fraud bagi seluruh pegawai. Tim Anti Fraud secara berkala melakukan sosialisasi terkait SAF. Untuk pelatihan digital fraud saat ini belum pernah dilaksanakan.”

It also appears that no specific training has yet been provided in this area, even though the Anti-Fraud Team has participated more frequently in training and certification activities. This shows that the scope of skill-based training for all employees is still quite limited. It is represented in the following statement:

“Untuk saat ini belum ada pelatihan khusus. Hanya saja untuk Tim Anti Fraud lebih sering mengikuti pelatihan baik secara offline atau online terkait SAF dibanding dengan pegawai di unit kerja lainnya. Untuk saat ini belum ada. Tapi kedepannya untuk bagian IT ataupun bagian terkait akan dilakukan sertifikasi berkala terkait keamanan sistem dan hal lain yang berkaitan... Saat ini belum ada dan rencananya akan diberikan pelatihan di tahun 2026.” (Chitra, 2025)

3. Lack of Digital Competency

Lack of digital competency was identified among some employees at PT BPR Bank Sleman, which may affect the implementation of anti-fraud strategy, specifically among digitisation trends that arises currently. Chitra (2025) pointed out that generational gap still exists in adapting to digitalization, where employees above the age of 45 tend to face greater difficulty in adjusting to digital processes than younger employees. This suggests that digital readiness among employees has not yet been evenly developed.

4. Low Understanding of Provisions

Chitra (2025) implied that many employees still do not fully understand the applicable regulations and policies. This condition may weaken the implementation of anti-fraud strategies as employees are expected to carry out their duties in accordance with those provisions.

5. Poor Training Design

Another deficiency could be found in the anti-fraud training design. It proves difficult to determine whether training has successfully increased employees' comprehension or capability due to the absence of clear indicators before and after training. Furthermore, the quality and applicability of the content presented may be diminished by the chosen speakers, who turns out, to be not always sufficiently knowledgeable in the relevant field (Chitra, 2025). This circumstance might make training less effective as a supportive tool for anti-fraud strategy implementation.

4.4.2 Implementation Barriers

Implementation barriers refer to obstacles encountered in practice during the execution of those strategies. These barriers were further explained, based on the findings, below:

1. Low Early Risk Awareness

Miharjo (2025) identified that one of the practical barriers lies in building early risk awareness across all employees, since

each work unit has different priorities and objectives. This condition makes fraud risk awareness difficult to internalize evenly and continuously across the Bank. Chitra (2025) similarly pointed out that employee awareness of fraud risk and the courage to report suspicious incidents are still lacking. These suggest that low early risk awareness remains a practical barrier because anti-fraud understanding has not yet been equally embedded across work units.

2. Hesitant to Use WBS

Dewi (2025) explained that, in practice, some employees are still afraid to use the whistleblowing system, especially when the report involves a superior, although anonymity and protection have already been socialized. Chitra (2025) also stated that employees are less likely to be aware of the whistleblowing system and remain afraid to disclose fraud or misconduct in their work unit. This indicated that the barrier might lie in employees' hesitation and fear despite the availability of the system itself.

3. Perceived Lack of Evidence to Report

Dewi (2025) outlined another implementation barrier, pointing out that reports lacking adequate evidence are challenging to investigate since they might merely seem like rumors or unsubstantiated allegations. This condition may discourage employees from reporting suspicious behavior when they believe

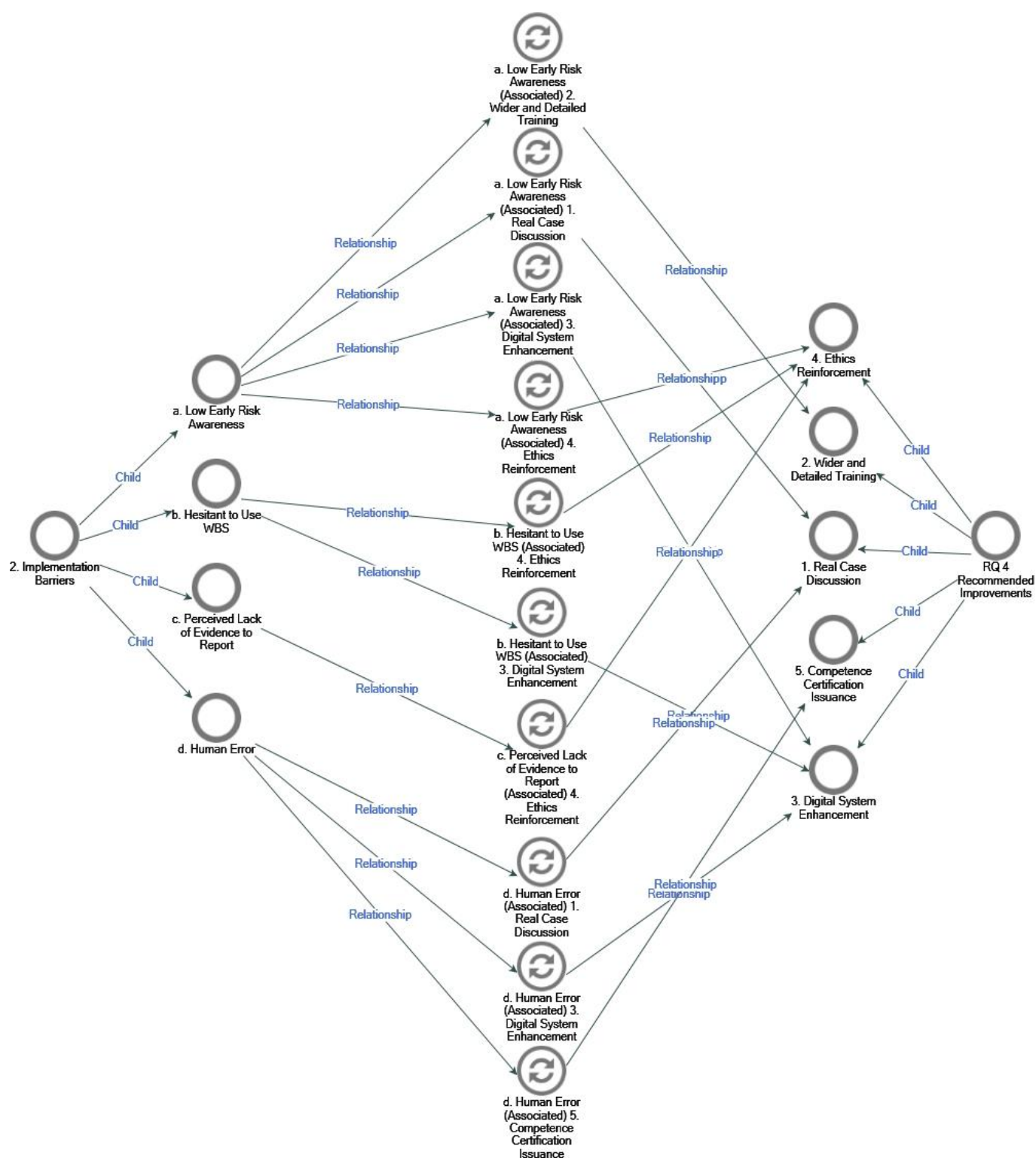
they lack sufficient evidence to support their concerns. As a result, the reporting process could be seen as challenging to start unless evidence is already available.

4. Human Error

Dewi (2025) noted that, regardless of how many systems and controls are established, fraud prevention still depends on the individuals involved, because people may eventually find gaps in the system. Chitra (2025) then showed that weak understanding of provisions, limited concentration during training, and uneven employee capability may also affect implementation. Taken together, these findings suggest that human error remains a barrier because anti-fraud implementation is influenced not only by formal controls, but also by the readiness, awareness, and conduct of employees themselves, as the first instrument in implementation itself.

4.5 Recommended Improvements Can be Made by PT BPR Bank Sleman

This section discusses the recommendations that may enhance the effectiveness of anti-fraud strategy implementation at PT BPR Bank Sleman in order to minimize occupational fraud. Based on the NVivo analysis, the recommended improvements include:



Source: Analyzed by The Researcher using NVivo 15

Figure 4.16 Analytical Map of Recommended Improvements in Enhancing Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

1. Real Case Discussion

One recommended improvement is the use of real case discussions in anti-fraud training. Referring to Setiawan (2025), in order to impart the information with greater detail, training may be accomplished through regular small group discussions or refreshment sessions rather than mass training. Similar to that, Dewi (2025) noted that anti-fraud socialization would be more effective if actual instances were utilized, especially internal fraud cases or similar cases from other banks, so that employees could comprehend the implications and applicability of fraud in actual situations. In addition, Chitra (2025) pointed out that a more engaging and grounded learning approach is required due to employees' poor comprehension of provision and their inability to focus during training, as well as the absence of clear training indicators. These statements imply that discussing actual cases could make the anti-fraud training more relevant, useful, and more memorable for employees.

2. Wider and Detailed Training

The interview findings indicated that, in order to prevent anti-fraud knowledge from being limited to specific functions, anti-fraud training still needs to be expanded in terms of employee coverage, and the material provided needs to be more comprehensive. Miharjo (2025) highlighted that stronger fraud risk awareness across work units still necessitates more detailed and comprehensive training. This training should also be given more widely across all work units and not just to Management Risk.

Consistent with this, Chitra (2025) observed that more SAF-related training is mostly received only by the Anti-Fraud Team rather than all employees in the Bank, and that particular training topic is still unavailable.

3. Digital System Enhancement

The current digital mechanism at PT BPR Bank Sleman still shows practical limitations in supporting anti-fraud implementation. Dewi (2025) explained that the existing web-based whistleblowing process remains inefficient, as mentioned in the prior section. As a result, digital system enhancement is recommended. According to Miharjo (2025), more effective digital applications are needed to help anticipate potential fraud more efficiently and to strengthen anti-fraud implementation.

4. Ethics Reinforcement

Behavioral factors remain a practical weakness in anti-fraud implementation, as explained in the prior section, which relates to employees' limited focus during training and lack of understanding of provisions (Chitra, 2025). Within this scope, ethics reinforcement is needed to build employees' ethical awareness that is more internalized and personally meaningful. Dewi (2025) noted that fraud prevention cannot rely solely on systems and controls, since individuals may still find gaps in the system over time. For this reason, reinforcement is also needed from the personal side, emphasizing more on the moral consequences of fraud. This reinforcement may also take place in the form of religious activities

so that anti-fraud awareness is not only understood formally, but also deeply rooted in the employees' daily activities.

5. Competence Certification Issuance

As highlighted before, limitations are still found in the formal competence development of personnel involved in anti-fraud implementation. Chitra (2025) indicated that all of the Anti-Fraud Team members should ideally participate in certification programs. However, this is still constrained by time limitations and the limited number of authorized institutions providing such certification. Therefore, competence certification issuance is recommended, as it may strengthen the capability and professionalism of the Anti-Fraud Team.

4.6 Conclusion

Based on the results of the data analysis and discussion, which were collected and processed using NVivo 15, it can be concluded that PT BPR Bank Sleman has implemented an anti-fraud strategy through four interrelated pillars. These pillars have been set up as a comprehensive control mechanism that focuses not only on handling fraud after it occurs but also on preventing, detecting, following up, and improving weaknesses in internal control. Furthermore, the findings indicate that PT BPR Bank Sleman's potential for occupational fraud falls into five categories, namely asset misappropriation, financial statement fraud, corruption, deception, and confidential information leakage.

The results also show that PT BPR Bank Sleman has implemented various anti-fraud measures under each of the four pillars. Under the prevention pillar, the

Bank performed anti-fraud awareness training, fraud risk identification, and know your employee procedures. Meanwhile, the detection pillar is being implemented through the surveillance system, surprise audit, and whistleblowing system. Furthermore, fraud indications are followed up through investigation, reporting to both internal and external related parties, and punishment will be imposed on the perpetrator. Lastly, the fourth pillar is reflected in monitoring, evaluation, and further action, which serve to assess implementation and support corrective improvement. These results imply that PT BPR Bank Sleman has established its anti-fraud strategy in a relatively structured manner. However, the implementation has not yet reached its full potential, as there are still a number of shortcomings and practical obstacles in the field.

The research then highlighted several deficiencies, including an ineffective whistleblowing mechanism, limited training scope, lack of digital competency, low understanding of provisions, and poor training design. Meanwhile, implementation barriers include poor early risk awareness, reluctance to use the whistleblowing system, a perceived lack of evidence to report in the whistleblowing system, and human error. These findings demonstrate that PT BPR Bank Sleman's problems are not just with systems and procedures but also with staff members' knowledge, skills, and readiness for putting anti-fraud strategies in place. In this sense, the anti-fraud mechanism's shortcomings seem to be a factor in the practical difficulties.

Based on these results, several suggested improvements can be made to increase the efficacy of PT BPR Bank Sleman's anti-fraud implementation. These include using actual case discussions in training, offering more comprehensive and

in-depth training that can be accessed by a broader scope within the organization, improving digital systems, reinforcing ethics, and issuing competency certifications for the Anti-Fraud Team. Therefore, it is clear that even though PT BPR Bank Sleman has previously adopted an anti-fraud strategy in an organized manner, additional development is still required to make the implementation more practical, effective, and flexible in reducing occupational fraud.

CHAPTER V

CONCLUSIONS AND SUGGESTIONS

This chapter covers the conclusions drawn from the research conducted. The conclusions are formulated based on the results of the analysis carried out through interviews with selected informants and documents referring to the research questions. Additionally, this chapter also discusses the limitations of the research and provides recommendations for future research.

5.1. Conclusions

The following are the conclusions drawn based on the findings of the research conducted:

1. The potential occupational fraud identified at PT BPR Bank Sleman can be classified into five categories, including asset misappropriation, corruption, financial statement fraud, deception, and leakage of confidential information, which were clearly stated in the guidelines of anti-fraud strategy implementation at PT BPR Bank Sleman as well as in the interviews. These fraud potentials reflect the vulnerability of banking operations involving fund management, lending activities, reporting, system access, and confidential information handling. This indicates that occupational fraud remains an issue that must be anticipated through structured internal control and anti-fraud strategy implementation.
2. The implementation of the anti-fraud strategy at PT BPR Bank Sleman had been arranged in a relatively structured manner. It reflected the four interrelated pillars, serving as a comprehensive fraud control system in

accordance with POJK Number 12/2024 concerning the Implementation of Anti-Fraud Strategy for Financial Services Institutions. Consequently, PT BPR Bank Sleman has its own internal guideline through Directors Regulation Number 21 of 2024 concerning the Guidelines for the Implementation of the Anti-Fraud Strategy of PT BPR Bank Sleman (Perseroda). The Anti-Fraud Strategy Team of PT BPR Bank Sleman has also been established based on Director's Decree Number 107/KPTS/DIR/2024, regulating the roles, duties, and team formation, which is directly responsible to the Director of Compliance. This demonstrates that PT BPR Bank Sleman had made an effort to reduce occupational fraud by implementing an extensive and integrated anti-fraud control system supported by internal governance structures.

3. The deficiencies identified were directly affected by the implementation barriers encountered in anti-fraud strategy implementation at PT BPR Bank Sleman. In this case, an ineffective whistleblowing mechanism contributed to employees' reluctance to use the system and to the perception that there was insufficient evidence to report because the reporting process was still seen as time-consuming. Likewise, low early risk awareness and human errors in implementation tended to be caused by the narrow scope of training, lack of digital competency, poor training design, and limited knowledge of the provisions. This illustrated that the obstacles PT BPR Bank Sleman faced were directly related to the weaknesses in the planning, execution, and support of the anti-fraud strategy.

4. The use of real case discussion was recommended due to the anti-fraud understanding among employees that still required practical reinforcement and refreshment. Wider scope and more detailed training were proposed because the current training remained limited to the Anti-Fraud Team and had not yet reached broader employees, which in turn contributed to low early risk awareness and competency gaps. Digital system enhancement was recommended since the Bank required more effective systems to anticipate fraud risks in an increasingly digital environment. Ethics reinforcement was suggested because human factors, such as hesitation to report and low sensitivity to fraud risk, remained significant barriers in implementation. Finally, competence certification issuance was proposed because the Anti-Fraud Team still required stronger professional capacity and official competency development in handling anti-fraud implementation. Thus, each recommendation was grounded in the specific identified challenges faced by PT BPR Bank Sleman in implementing anti-fraud strategies.

5.2 Limitations

In conducting this research, the researcher identified several limitations as follows:

1. This research was conducted only at PT BPR Bank Sleman. Hence, the findings reflected the conditions and implementation context of one rural bank and cannot be generalized directly to other BPRs or financial institutions.

2. The annual report used in this research was the 2024 Annual Report, since the 2025 Annual Report had not been published at the time the research was conducted.
3. The analysis relied mainly on interview data and the accessible documents during the research process. As a result, the findings were dependent on the availability of information provided by the informants and supporting documents obtained during the research. Therefore, it did not quantitatively represent the direct effectiveness of the anti-fraud strategy in minimizing fraud incidents over time.

5.3 Suggestions

Based on the research that had been conducted, the researcher provide the following suggestions:

1. For PT BPR Bank Sleman, the implementation of the anti-fraud strategy should be further strengthened through improvements to the whistleblowing process, broader scope, and comprehensive anti-fraud training, periodic digital system upgrade, ethics reinforcement, and competency development for the Anti-Fraud Team. These initiatives are essential for ensuring that anti-fraud strategies are successfully applied in daily operations, besides being officially developed.
2. For future researchers, similar research may be conducted in other BPRs or financial institutions to serve as a comparative study of the anti-fraud strategy implementation across various organizational contexts. Future research may also integrate qualitative and quantitative methods to examine

the anti-fraud strategy implementation along with its contribution in reducing fraud incidents and improving the efficacy of internal controls.

BIBLIOGRAPHY

- ACFE. (2024). *Occupational fraud 2024: A report to the Nations*.
- Akanfe, O., Bhatt, P., & Lawong, D. A. (2025). Technology Advancements Shaping the Financial Inclusion Landscape: Present Interventions, Emergence of Artificial Intelligence and Future Directions. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-025-10597-z>
- Apsari, H. L., & Chariri, A. (2025). The Determinants of Occupational Fraud: An Analysis Using The New Fraud Star Theory. *Jurnal Akademi Akuntansi*, 8(3), 356–380. <https://doi.org/10.22219/jaa.v8i3.37258>
- Arens, A. A., Randal, J. E., & Mark, S. B. (2015). *Auditing dan jasa assurance pendekatan terintegrasi* (15th edn, Vol. 1). Erlangga.
- Bakri, A. A., Hasanah, N., & Lasmiatun, K. (n.d.). Financial Technology Innovation and Banking Industry Transformation (a Literature Study on Financial Markets). *MULTIFINANCE Jurnal Ekonomi, Manajemen Dan Perbankan*, 230–238. Retrieved <http://altinriset.com/journal/index.php/multifinance/article/view/112/95>
- Bank Indonesia. (2011). *Surat edaran Bank Indonesia nomor 13/28/DPNP tentang penerapan strategi anti-fraud bank umum* (Circular Letter 13/28/DPNP; Surat Edaran Bank Indonesia). Bank Indonesia. <https://ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-bank-indonesia/Pages/surat-edaran-bank-indonesia-nomor-13-28-dpnp.aspx>
- Bank Sleman. (2025a, August 30). Bank Sleman meraih penghargaan the best performance BPR 2025 dalam ajang Infobank rural bank award tahun 2025. *Bank Sleman*. <https://banksleman.co.id/2025/08/30/bank-sleman-meraih-penghargaan-the-best-performance-bpr-2025-dalam-ajang-infobank-rural-bank-award-tahun-2025/>
- Bank Sleman. (2025b, November 27). Bank Sleman menyabet tiga penghargaan dalam acara anugerah keterbukaan informasi badan publik DIY tahun 2025. *Bank Sleman*. <https://banksleman.co.id/2025/11/27/bank-sleman-menyabet-tiga-penghargaan-dalam-acara-anugerah-keterbukaan-informasi-badan-publik-diy-tahun-2025/>
- Baxter, P., & Jack, S. (2015). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*. <https://doi.org/10.46743/2160-3715/2008.1573>
- Breuer, W., & Knetsch, A. (2023). Recent Trends in the Digitalization of Finance and Accounting. *Journal of Business Economics*, 93(9), 1451–1461. <https://doi.org/10.1007/s11573-023-01181-5>
- Buchholz, A. K. (2012). *SAS 99: Deconstructing the Fraud Triangle and Some Classroom Suggestions*.
- Butcovan, A. (2015). *Banking Security in the Context of International Relations*. (3).
- Cheliatsidou, A., Sariannidis, N., Garefalakis, A., Azibi, J., & Kagias, P. (2023). The International Fraud Triangle. *Journal of Money Laundering Control*, 26(1), 106–132. <https://doi.org/10.1108/JMLC-09-2021-0103>

- Cressey, D. R. (1953). *Other people's money: A study of the social psychology of embezzlement*. <https://psycnet.apa.org/record/1954-06293-000>
- Duffield, G. M., & Grabosky, P. N. (2001). *The psychology of fraud*. Australian Institute of Criminology. <https://www.aic.gov.au/publications/tandi/tandi199>
- Fadli, M. R. (2021). Memahami Desain Metode Penelitian Kualitatif. *HUMANIKA*, 21(1), 33–54. <https://doi.org/10.21831/hum.v21i1.38075>
- Fajri, K. F., & Prabowo, H. Y. (2024). Fraud Threats: How Organization Improves the Anti-Fraud Team Quality? *Jurnal Akuntansi & Auditing Indonesia*, 28(1), 95–103. <https://doi.org/10.20885/jaai.vol28.iss1.art10>
- Fajria, F. (2023). *Penerapan strategi anti fraud dalam meminimalkan occupational fraud pada pt bank x cabang kota tarakan*. Universitas Islam Indonesia.
- Gupta, M., & Gupta, R. (2025). Corporate Financial Fraud: A Conceptual and Qualitative Analysis of Financial Statements Manipulation. *VEETHIKA-An International Interdisciplinary Research Journal*, 11(3), 27–38. <https://doi.org/10.48001/veethika.1103003>
- Hai-Jew, S. (2019). *Matrix queries and matrix data representations in NVivo 12 plus*. <https://idme-test.ome.ksu.edu/MatrixQueries.pdf>
- Hammersley, M. (2013). *What is qualitative research?* Bloomsbury.
- Hana, M. Z. (2023). *Penerapan strategi anti fraud dalam meminimalkan occupational fraud pada pt bpr danagung bakti yogyakarta*. Universitas Islam Indonesia.
- Hancock, D. R., & Algozzine, R. (2006). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.
- Hidajat, T. (2020). Rural Banks Fraud: A Story from Indonesia. *Journal of Financial Crime*, 27(3), 933–943. <https://doi.org/10.1108/JFC-01-2020-0010>
- Kamdjoung, J. R. K., Sando, H. D., Kala, J. R., Teutio, A. O. N., Tiwari, S., & Wamba, S. F. (2024). Data Analytics-Based Auditing: A Case Study of Fraud Detection in the Banking Context. *Annals of Operations Research*, 340(2–3), 1161–1188. <https://doi.org/10.1007/s10479-024-06129-8>
- Kardiman, T. A., M, R. Y., & Indriani, F. (2025). Digital Transformation Sustainability in Indonesia's Banking Sector: A Systematic Review. *Arthatama Journal of Business Management and Accounting*, 9(2), 258–277.
- Kemendagri RI. (2024). *Permendagri number 21 year 2024 (21/2024)*. <https://peraturan.bpk.go.id/Details/321679/permendagri-no-21-tahun-2024>
- Kennedy, P. S. J., & Siregar, S. L. (2017). *Para Pelaku Fraud Di Indonesia Menurut Survei Fraud Indonesia*.
- Korstjens, I., & Moser, A. (2018). Series: Practical Guidance to Qualitative Research. Part 4: Trustworthiness and Publishing. *European Journal of General Practice*, 24(1), 120–124. <https://doi.org/10.1080/13814788.2017.1375092>

- Leavy, P. (Ed.). (2014). *The Oxford handbook of qualitative research* (1st edn). Oxford University Press.
<https://doi.org/10.1093/oxfordhb/9780199811755.001.0001>
- Mabior, M. M., & Wanyama, K. W. (2024). Role of Forensic Investigations in Reduction of Financial Fraud Among Commercial Banks in South Sudan. *International Journal of Finance and Accounting*, 3(1), 1–14.
<https://doi.org/10.37284/ijfa.3.1.1845>
- Matthew, K., Patrick, K., & Denise, K. (2013). *The Effects of Fraudulent Procurement Practices on Public Procurement Performance*. 3.
https://www.researchgate.net/publication/236208095_The_Effects_of_Fraudulent_Procurement_Practices_on_Public_Procurement_Performance
- Miharjo, D. H. (2018). *Kajian Optimalisasi Auditor Internal Dalam Penerapan Sistem Anti Fraud*.
- Miles, M. B., Huberman, A. M., & J., S. (2014). *Qualitative data analysis: A methods sourcebook* (3rd edn). SAGE Publications.
- Nawawi, A., & Salin, A. S. A. P. (2018). Internal Control and Employees' Occupational Fraud on Expenditure Claims. *Journal of Financial Crime*, 25(3), 891–906. <https://doi.org/10.1108/JFC-07-2017-0067>
- Oboh, C. S. (2023). Emotional Intelligence and Fraud Tendency: A Survey of Future Accountants in Nigeria. *European Journal of Management Studies*, 28(1), 3–22. <https://doi.org/10.1108/EJMS-05-2022-0038>
- OJK. (2015). *POJK nomor 13/POJK.03/2015* (13/POJK.03/2015). <https://peraturan.bpk.go.id/Details/128844/peraturan-ojk-no-13poj032015-tahun-2015>
- OJK. (2024). *POJK nomor 12 tahun 2024 tentang penerapan strategi anti fraud bagi lembaga jasa keuangan* (POJK 12/2024). <https://peraturan.go.id/files/peraturan-ojk-no-12-tahun-2024.pdf>
- OJK. (2025). *Profil entitas BPR konvensional Q4-2019 s/d Q2-2025* [Data set]. <https://data.ojk.go.id/SJKPublic/Dataset/Dataset/Dataset/1>
- Olsen, W. (2004). *Triangulation in Social Research: Qualitative and Quantitative Methods Can Really Be Mixed*.
- Peltier-Rivest, D. (2009). An Analysis of the Victims of Occupational Fraud: A Canadian Perspective. *Journal of Financial Crime*, 16(1), 60–66.
<https://doi.org/10.1108/13590790910924966>
- Petersen, A., Bruwer, J.-P., & Roux, S. L. (2018). *Occupational Fraud Risk, Internal Control Initiatives and the Sustainability of Small, Medium and Micro Enterprises in a Developing Country: A Literature Review*. 14(4).
- Prabha, M., Sharmin, S., Khatoon, R., Imran, M. A. U., & Mohammad, N. (2024). Combating Banking Fraud with It: Integrating Machine Learning and Data Analytics. *THE AMERICAN JOURNAL OF MANAGEMENT AND ECONOMICS INNOVATIONS*, 06(07), 39–56.
<https://doi.org/10.37547/tajmei/Volume06Issue07-04>
- Priyatni, E. T., Suryani, A. W., Fachrunnisa, R., Supriyanto, A., & Zakaria, I. (2020). *Pemanfaatan NVivo dalam penelitian kualitatif: NVivo untuk kajian pustaka, analisis data, dan triangulasi*. Pusat Pendidikan Lembaga

- Penelitian dan Pengabdian Kepada Masyarakat (LP2M) Universitas Negeri Malang (UM). <https://fip.um.ac.id/wp-content/uploads/2021/10/b5-Pemanfaatan-NVIVO-dalam-Penelitian-Kualitatif.pdf>
- PT BPR Bank Sleman. (2024a). *Keputusan direksi PT BPR bank sleman nomor 107/KPTS/DIR/2024 tentang tim penerapan strategi anti fraud PT BPR bank sleman (perseroda)* (Keputusan Direksi Nomor 107/KPTS/DIR/2024). PT BPR Bank Sleman.
- PT BPR Bank Sleman. (2024b). *Pedoman penerapan strategi anti fraud PT BPR Bank Sleman (Perseroda)* (21/PERDIR/BS/2024).
- PT BPR Bank Sleman. (2024c). *PT BPR Bank Sleman annual report 2024*. <https://banksleman.co.id/lap-tahunan/laporan-tahunan-2024/>
- Putri, A. (2012). Kajian: Fraud (Kecurangan) Laporan Keuangan. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, 3(1), 13–22. <https://doi.org/10.33558/jrak.v3i1.142>
- Ramli, R. R. (2024). [Review of *Kaleidoskop 2024: BPR ‘gulung tikar’ naik 5 kali lipat*, by E. Djumena]. *Kompas.com*. <https://money.kompas.com/read/2024/12/29/161600426/kaleidoskop-2024-bpr-gulung-tikar-naik-5-kali-lipat?page=all>. Membership: <https://kmp.im/plus6> Download aplikasi: <https://kmp.im/app6>
- Rustiarini, N. W., Suryandari, N. N. A., & Nova, I. K. S. (2016). Red Flags and Fraud Prevention on Rural Banks. *Buletin Ekonomi Moneter dan Perbankan*, 19(2), 177–206. <https://doi.org/10.21098/bemp.v19i2.629>
- Saputra, A. (2017). *Pengaruh Sistem Internal, Kontrol, Audit Internal Dan Penerapan Good Corporate Governance Terhadap Kecurangan (FRAUD) Perbankan (Studi Kasus Pada Bank Syariah Anak Perusahaan BUMN di Medan)*. 1(1). <https://owner.polgan.ac.id/index.php/owner/article/view/15/8>
- Sawyer, L., Dittenhofer, M. B., & Schiner, J. H. (2005). *Sawyer’s internal auditing: Audit internal sawyer* (5th ed). Salemba Empat.
- Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed). Wiley.
- Shanikat, M., Al-Farah, A., & Dorgham, T. H. (2014). *Occupational Fraud Prevention Mechanisms: Jordanian Companies Experience*.
- Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information*, 22(2), 63–75. <https://doi.org/10.3233/EFI-2004-22201>
- Sudarmo, Sawardi, T., & Yulianto, A. (2008). *Fraud auditing* (R. Lestari, Ed.; 5th ed). Pusat Pendidikan dan Pelatihan Pengawasan - Badan Pengawasan Keuangan dan Pembangunan.
- Suhartono, S. (2016). Komite Anti Fraud: Solusi Menuju Zero Fraud. *Jurnal Akuntansi*, 5(1), 90–104. https://www.researchgate.net/profile/Sugi-Suhartono/publication/336230834_KOMITE_ANTI_FRAUD_SOLUSI_MENUJU_ZERO_FRAUD/links/5d9581ada6fdccfd0e7137ef/KOMITE-ANTI-FRAUD-SOLUSI-MENUJU-ZERO-

- FRAUD.pdf?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
- Vanini, P., Rossi, S., Zvizdic, E., & Domenig, T. (2023). Online Payment Fraud: From Anomaly Detection to Risk Management. *Financial Innovation*, 9(1), 66. <https://doi.org/10.1186/s40854-023-00470-w>
- Wang, Y., Ashton, J. K., & Jaafar, A. (2019). Money Shouts! How Effective Are Punishments for Accounting Fraud? *The British Accounting Review*, 51(5), 100824. <https://doi.org/10.1016/j.bar.2019.02.006>
- Wang, Y., Ashton, J. K., & Jaafar, A. (2023). Financial Statement Fraud, Recidivism and Punishment. *Emerging Markets Review*, 56, 101033. <https://doi.org/10.1016/j.ememar.2023.101033>
- Yanti, S. R., & Hidayah, N. (2023). Pengaruh Implementasi Good Corporate Governance, Kompetensi Auditor Internal dan Efektivitas Pengendalian Internal Terhadap Kecurangan Praktik Perbankan dengan Whistleblowing System Sebagai Variabel Moderasi: Studi Kasus PT Bank Mandiri (persero) Tbk Area Pluit Selatan Jakarta Utara. *Owner*, 7(2), 974–985. <https://doi.org/10.33395/owner.v7i2.1376>

APPENDICES

Appendix 1. Certificate of Research Completion



SURAT KETERANGAN

Nomor : 75/SK/BS/IV/2026

Yang bertanda tangan di bawah ini :

Nama : Rizky Chitra E, S.Psi
 Jabatan : Human Capital Officer
 Alamat : PT BPR Bank Sleman (Perseroda)
 Jl. Magelang Km. 10, Tridadi, Sleman

Dengan ini menerangkan bahwa :

Nama : Chantika Rahma Agustina
 No. Mahasiswa : 22312185
 Program Studi : Akuntansi International Undergraduate Program
 Fakultas : Fakultas Bisnis dan Ekonomika
 Universitas : Universitas Islam Indonesia

Telah melakukan penelitian di PT BPR Bank Sleman (Perseroda) untuk penulisan Skripsi dengan judul **"An Analysis of The Anti-Fraud Strategies Impelementation in Minimizing Occupational Fraud at PT BPR Bank Sleman"** pada bulan November 2025 s/d Februari 2026.

Guna melengkapi perpustakaan PT BPR Bank Sleman (Perseroda), maka mahasiswa yang bersangkutan agar menyampaikan 1 (satu) eksemplar copy hasil Skripsi yang telah disetujui.

Demikian surat keterangan ini kami buat untuk dipergunakan semestinya.

Dikeluarkan di : Sleman
 Pada tanggal : 20 April 2026



Appendix 2. Interview Transcript 1

Interviewee : Mr. Dwi Handoyo Miharjo

Interview Date : 9 December 2025

Position : Risk Management Staff

R : Researcher

I : Interviewee/Informant

R : Kalau di PT BPR Bank Sleman sendiri, untuk digitalisasinya sudah sejauh mana ya, Pak?

I : Namanya di perbankan yah, otomatis digitalisasi kita selalu *develop*, kita selalu tingkatkan, berkembang. Jadi secara *core banking*, secara sistem operasional, bahkan secara *manage human resource* gitu, hampir semuanya kita menggunakan digitalisasi. Bahkan terkait dengan *report*, laporan, dan lain-lain. Nah, yang terbaru, kita juga telah membuat ATM seperti itu, seperti bank pada umumnya ya. Ada ATM, kemudian kita sedang mengembangkan *mobile banking* kita juga. Kemudian, kita juga kerja sama dengan *switching-switching* yang sudah terkenal seperti ALTO, seperti Prima. Jadi saya rasa ini adalah bentuk layanan, karena perbankan itu layanan kepada masyarakat atau kepada nasabah. Jadi, ya tentu digitalisasi itu sangat penting dan saya rasa semua personal yang menggunakan digitalisasi itu lebih efektif dan lebih efisien.

R : Kalau untuk sistem atau aplikasi digital yang mendukung proses pencegahan dan deteksi *fraud* ada, Pak?

I : Oke, jadi kalau untuk *fraud*, tentu kita dari *core banking* itu sudah ada parameter-parameternya, *red flag*-nya juga sudah ada. Kemudian kita juga punya *audit trail*-nya ya. Jadi, kita melihat sistem ini digunakan oleh siapa saja, yang mengakses sistem itu siapa saja, sehingga ada transaksi-transaksi atau yang masuk ke dalam sistem yang mencurigakan itu bisa diketahui. Kemudian di sisi lain, kita juga punya namanya FDS. FDS itu *Fraud Detection System*. Jadi, *Fraud Detection System* ini berfungsi untuk menganalisa atau menetapkan hal-hal yang di luar batas normal. Jadi itu *parameterized* ya, jadi itu ada parameternya. Parameternya itu misalnya seperti, oh ada transaksi ATM dilakukan secara bersamaan di selang waktu bersamaan, gitu. Jadi, itu FDS kita ngebaca itu, sistem kita ngebaca itu. Atau misalnya ada bukan nasabah tapi berhasil melakukan transaksi seperti itu. Atau ada rekening pasif tapi dapat melakukan transaksi. Jadi hal-hal yang tidak normal itu akan diketahui oleh FDS namanya, *Fraud Detection System*.

R : Kalau untuk di divisi Bapak sendiri, apakah sering menerima pelatihan tentang risiko *fraud* digital?

I : Oh ya, tentu. Jadi kalau *fraud* digital, karena divisi saya kan *risk management* ya. Departemen *Compliance* atau Kepatuhan. Saya jadi unit *risk management*. Lima tahu saya di *risk management*, kita otomatis setiap satu tahun, satu kali itu akan ada pelatihan terkait dengan *fraud*. *Every fraud*. Jadi bukan cuma *fraud* terkait dengan uang, tapi *fraud* bagaimana pembocoran data, rahasia data, dan lain-lain. Selain itu, kita juga bukan hanya mendapatkan edukasi, kita juga memberikan edukasi ke unit kerja lainnya atau departemen lainnya. Di departemen saya, kebetulan itu, juga turut menyampaikan atau mensosialisasikan terkait dengan

fraud prevention. Artinya, pencegahan *fraud* ya. Nah itu yang kita pengen, apa, tujuannya adalah kita pengen untuk teman-teman itu bisa sadar risiko sejak dini. Karena kebanyakan kan, orang-orang tau *fraud* itu, oke saya nyuri uang, saya mengatakan itu *fraud*. Tapi, *fraud* kan bukan cuma itu saja. Mungkin nanti mbak juga bisa mencari jawabannya, *fraud* itu apa saja. Tapi, misalnya kamu pembocoran rahasia, ada benturan kepentingan, itu sudah merenan ke area *fraud*. Jadi, itu menurut saya penting diketahui oleh seluruh unit kerja, bukan cuma unit saya sendiri.

R : Kalau menurut Bapak sendiri, ancaman *fraud* yang paling relevan saat ini di BPR Bank Sleman itu apa ya, Pak?

I : Oke, yang paling relevan sebenarnya potensi risiko itu kapan saja bisa datang ya. Secara risiko *fraud* itu sebenarnya ada dua, ada dua poin. Yang pertama adalah *human error* dan *system error*. Kalau menurut saya cuma dua itu. Nah, kalau *human error* artinya kan *fraud* itu terjadi karena kompetensi si *human*-nya, si manusianya. Entah itu dia tidak mengetahui, oh ternyata saya melanggar dan itu merugikan pihak bank, itu bisa jadi memang penyalahgunaan dan ketika orang tersebut mendapatkan keuntungan secara pribadi, itu bisa kita katakan *fraud*. Nah, kemudian kalau *system error* ini lebih ke macam-macam ya. Jadi, entah itu kalau zaman sekarang itu mungkin *cyber security* yang kurang kuat, kemudian ada *hacker* dari pihak eksternal, nah itu kan berkaitan dengan sistem. Jadi, bagaimana kita menjaga sistem itu agar bisa tetap mengantisipasi hal-hal yang memungkinkan terjadinya *fraud*.

R : Misal ada indikasi munculnya *fraud*, bagaimana langkah-langkahnya dalam mengatasi hal tersebut?

I : Oke, langkah-langkahnya ya. Yang pertama kita ada beberapa langkah. Satu itu adalah kita punya namanya *whistleblower*. *Whistleblower* itu apa, jadi rekan-rekan kerja kita yang mengetahui indikasi *fraud* dengan bukti awal, itu kita mempersilahkan melaporkan ke unit kerja yang telah ditunjuk. Otomatis kerahasiaannya dari pegawai tersebut akan kami jamin seribu persen. Oke, kemudian nanti ada timnya tersendiri ketika laporannya sudah masuk, nanti akan ada tim *investigation* yang akan mengurus hal tersebut. Nah, yang kedua bagaimana kalau misalnya terjadi *fraud*, tadi kan saya bilang ada FDS ya, *Fraud Detection System*. Nah, ketika ada hal-hal indikasi, wah ternyata ada hal-hal yang nggak wajar nih, nah itu kita lakukan analisa juga. Itu tidak perlu pakai *whistleblower*, karena pihak eksternalnya. Jadi, kita menganalisa kalau misalnya memang ada hal-hal dirasa mencurigakan, kita akan melakukan prosedur-prosedur yang telah ditetapkan. Jadi ada sih mbak, hal-hal yang memang kita itu sudah punya prosedur untuk bagaimana sih kalau misalnya indikasi *fraud*-nya itu muncul atau misalnya ada terjadi *fraud*. Nah, di sisi lain kita juga kan di bawah regulator OJK dan BI. Nah, kalau untuk OJK itu juga kita punya kewajiban untuk melaporkan seluruh kejadian *fraud* dan itu secara rutin. Walaupun di periode tersebut tidak ada kejadian *fraud*, kita harus tetap melaporkan pelaporan anti *fraud* secara nihil karena memang tidak ada, tapi pelaporannya harus tetap jalan. Nah, di BI pun seperti itu.

R : Untuk *whistleblower* tadi yang mengelola siapa ya, Pak?

I : Kalau *whistleblower* itu memang kita ada namanya Tim Anti *Fraud*. Di Bank Sleman itu ada Tim Anti *Fraud*. Nah, Tim Anti *Fraud* itu lintas unit kerja. Lintas unit kerja. Nah, yang mengelola *whistleblower* itu nanti memang ditunjuk adalah dari unit SDM.

R : Kalau tadi untuk Tim Anti *Fraud* itu kan lintas divisi begitu Pak, untuk pemilihannya itu apakah ada mekanismenya, Pak?

I : Pemilihannya ya? Kalau pemilihannya tidak ada mekanisme, cuman kita akan melibatkan unit-unit yang memang dirasa berwenang untuk mengurus hal tersebut. Karena kalau pakai mekanisme, takutnya unit yang tidak ada kaitannya malah bisa masuk dalam Tim Anti *Fraud* itu. Contoh, unit umum masuk Tim Anti *Fraud*, ya mungkin bisa bisa aja, tapi dia tidak berkompeten di situ. Sehingga unit yang berkompeten seperti apa? Contoh tim audit, Satuan Kerja Audit Internal, Satuan Kerja Manajemen Risiko, kemudian SDM yang mengelola ini, dan *Compliance*. Jadi unit-unit yang terkait lah, unit-unit yang mungkin kira-kira memang akan berurusan dengan *fraud*.

R : Untuk unit kerja *Management Risk* sendiri bagaimana koordinasinya dengan *Internal Audit*?

I : Koordinasinya ya? Oke, kalau koordinasi terkait dengan *Internal Audit*, kita koordinasi paling secara langsung ya. Memang kita beda departemen, jadi kalau audit itu departemennya langsung dia di pusat, di direktur utama, kalau kami kan di *compliance director*. Jadi kita di direktur kepatuhan. Jadi kita koordinasi biasa secara langsung aja, kita surat-menyurat, kemudian tim audit pun itu melakukan pemeriksaan ke SKMR. Jadi kita juga bagian dari pemeriksaan tim audit, kemudian

kadang kita juga ada data-data dari SKMR yang diminta oleh tim audit secara bersurat. Jadi ya koordinasinya nggak ada koordinasi khusus, cuma memang langsung saja.

R : Untuk hasil dari *Fraud Detection System* itu, apakah itu kewajiban dari unit *Management Risk* untuk melaporkan itu secara berkala ke *Internal Audit*?

I : Untuk *Fraud Detection System* ketika dilakukan analisa dan itu memang benar terjadi kecurangan, nah itu memang kita akan langsung sampaikan ke audit. Tapi kalau misalnya tidak, artinya *stop* sampai di SKMR saja. Sampai di *Management Risk* saja.

R : Kalau untuk *risk register* sendiri apakah selalu diperbarui?

I : *Risk register*? Oke, mantap nih pertanyaannya. Jadi *risk register* kita diperbarui, jadi setiap bulan kita, teman-teman itu mengisi *risk register* yang ada di seluruh unit kerja, mereka setiap bulan mengisi, meskipun memang ada beberapa unit kerja itu kadang kelewat ya mengisinya, cuman tetap mengisi secara bulanan.

R : Di departemen *Management Risk* itu, kira-kira apa saja yang sering dilakukan untuk meningkatkan SDM di departemen itu sendiri, Pak?

I : Khusus SDMnya *Management Risk* ya? Jadi khusus departemen *Management Risk*, kita memang dibekali ya oleh SDM dan oleh perusahaan, jadi yang pertama kita pasti akan selalu diikutkan pelatihan-pelatihan yang berbau *fraud*, kemudian berbau audit, kemudian berbau terkait dengan *compliance* atau kepatuhan, jadi kemudian juga ada namanya APU-PPT, nah itu ita diikutkan pelatihan itu secara

rutin secara konsep. Tujuannya apa? Tujuannya untuk meningkatkan kompetensi dari pegawai itu sendiri.

R : Menurut Bapak sendiri untuk pelatihan tersebut, apakah sudah efektif dalam menunjang kinerja?

I : Oh iya, kalau efektif, efektif, itu sangat membantu, karena ada hal-hal yang memang kita tidak bisa, misalnya kita belum tahu jadi tahu, atau mungkin ada aplikasi yang belum kita gunakan, di pelatihan tersebut ada penawaran aplikasi yang bermanfaat bagi kita, itu kita gunakan. Jadi itu sangat efektif.

R : Kalau untuk kendala sendiri, seringnya apa yang dihadapi oleh departemen Bapak?

I : Oke, jadi kalau untuk di *Management Risk*, kendalanya itu sebenarnya ini ya, jadi bagaimana upaya untuk membuat kesadaran risiko sejak dini di seluruh karyawan. Nah itu akan menjadi pr juga, karena seluruh karyawan ini kan tujuannya berbeda-beda. Contoh misalnya *Marketing*, tujuannya target. Contoh Umum, tujuannya bagaimana operasional kantor berjalan dengan baik. Nah, ketika kita menetapkan risiko di seluruh unit kerja, itu mungkin mereka memahami dan melaksanakan. Tetapi untuk secara keberlangsungan, untuk oh ini berisiko tinggi, ini berisiko itu, mungkin kita masih butuh upaya untuk mengoptimalkan ya. Jadi, belum seratus persen saya sampaikan terkait dengan tingkat kesadaran risiko. Nah itu yang menjadi pr sih bagi kita.

R : Di Bank Sleman sendiri, biasanya apa yang dilakukan untuk meningkatkan kesadaran anti *fraud*?

I : Ya, jadi kalau untuk meningkatkan kesadaran dari anti *fraud*, kita setiap bulan itu melakukan kunjungan ya, kunjungan ke seluruh departemen untuk mensosialisasikan terkait dengan *fraud prevention*. Nah disitu kita jelaskan termasuk tadi *whistleblowing* dan lain-lain, itu kita jelaskan di setiap bulan itu di unit kerja berbeda masing-masing. Kenapa kita tidak kumpulkan dalam satu ruangan secara bersama-sama? Karena kami pengen lebih dekat sama per unit kerjanya. Saya rasa itu lebih efektif. Yang kedua memang secara umum, itu setiap tahun sudah ada terkait dengan *fraud*, sosialisasi juga. Selain itu kita juga ada yang namanya tanda tangan pakta integritas atau tanda tangan anti *fraud* untuk pegawai. Sehingga itu kita perbaharui selama 1 tahun sampai 6 bulan sekarang.

R : Kalau tadi di Tim Anti *Fraud* itu kan lintas unit ya Pak, itu biasanya berapa anggota, Pak?

I : Timnya? Timnya itu seluruh unit kerjanya. Misalnya di saya ada 3 orang, yaudah 3 orang itu masuk sebagai Tim Anti *Fraud*.

R : Kalau pembagian tugas di Tim Anti *Fraud* dalam menangani *fraud* itu sendiri seperti apa, Pak?

I : Oke, jadi beda-beda ya memang tugasnya. Kalau *Management Risk* itu bertugasnya adalah *prevention*-nya. Jadi *before*-nya, *before* terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk *fraud* itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatornya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan *whistleblower*-nya, nanti *punishment*-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau

Compliance itu nanti di ketentuannya. Apakah *fraud* ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.

R : Untuk peluang *fraud* itu Pak, kira-kira apa yang paling berpotensi untuk memicu munculnya *fraud*, mungkin dari adanya kelemahan kontrol atau lain-lain?

I : Jadi *Alhamdulillah*, *fraud* di kita itu kan memang sangat jarang terjadi ya. Kontrol kita kemungkinan besar walaupun itu terjadi, artinya itu dari *human*-nya memang. *Human*-nya artinya mungkin dari apa? Mungkin dari kontrol kita yang kurang. Nah, itu yang kita selalu benahi. Jadi memang benar apa yang mbak sampaikan, pengawasan melekat, ketentuan, kontrol internal, sistem kontrol, itu yang menjadi pintu pencegahan kita untuk mengantisipasi terjadinya *fraud* itu.

R : Untuk sistem evaluasi dari Tim Anti *Fraud* itu, apakah ada KPI-nya, Pak?

I : Kalau untuk Anti *Fraud* itu nanti KPI-nya setahu saya bukan KPI atas nama Anti *Fraud*-nya, tapi KPI personalnya. Jadi KPI-nya itu lebih ke arah misalnya SKMR secara personal, KPI-nya sudah bagus, mengantisipasi hal-hal terjadinya *fraud*. Oh, Audit telah melakukan investigasi. Jadi per unit kerjanya ya, bukan Tim Anti *Fraud*-nya. Nah, untuk yang melakukan *fraud*-pun pasti tentu ada KPI-nya juga. Misalnya kamu melakukan *fraud*, otomatis KPI-mu akan turun.

R : Berarti per individual begitu ya, Pak?

I : Yes, betul.

R : Apakah ada rekomendasi untuk meningkatkan kualitas SDM di *Management Risk* sendiri, Pak?

I : Rekomendasi untuk di *Management Risk* tentu kita ingin mendapatkan pelatihan-pelatihan yang lebih detail lagi, lebih dalam lagi, bahkan mungkin kita membutuhkan aplikasi-aplikasi yang tadi kan mbak sudah menyinggung digitalisasi di awal. Mungkin aplikasi secara digital yang lebih efektif lagi. Jadi kita bisa mengantisipasi hal-hal potensi terjadinya kecurangan itu. Nah, di sisi lain memang *fraud* itu bukan cuman dari, yang bukan cuman diketahui oleh unit kami, unit *Management Risk*. Tapi harapannya kami juga ingin pelatihan lebih detail juga itu disampaikan ke seluruh unit kerja.

R : Kalau untuk digitalisasi sendiri, kan tadi udah lumayan banyak ya Pak di sini. Kira-kira ada gap gitu nggak di antara karyawan, di antara pegawai itu? Ada gap dalam penggunaan digital?

I : Oke, kalau untuk gap saya rasa secara umum, digital secara umum nggak ada ya. Jadi misalnya terkait dengan ATM, semua orang bisa menggunakan ATM gitu. Kemudian misalnya *mobile banking*, semua orang bisa menggunakan *mobile banking*. Nah, yang jadi masalah kan, kalau misalnya ada, kadang-kadang kita di mesin ATM, uangnya saldonya berkurang, uangnya tidak keluar gitu misalnya. Nah, itu kan semua orang tau cara mengantisipasinya bagaimana gitu. Nah, itu yang tau itu kan Tim IT atau Tim *Accounting* kita, jadi ada dinamakan rekonsiliasi. Nah, jadi sebenarnya bukan gap, tapi memang kita mengetahui digitalisasi itu sesuai dengan porsi unit kerja masing-masing. Jadi, ketika kamu memang di bagian *front line*, kamu harus tau terkait dengan digitalisasi di bagian *front line*. *It's a must* gitu ya, maksudnya itu kewajiban gitu. Nah, kemudian kalau misalnya kamu di *Management Risk*, kamu harus punya kewajiban terkait dengan memahami FDS,

Fraud Detection System. Misalnya kamu di Audit, kamu harus memahami *audit trail* kita. Jadi, setiap unit memiliki digitalisasinya masing-masing lah.

R : Berarti untuk di unitnya sendiri, biasanya semua orang sudah paham gitu ya, Pak?

I : Sudah paham dan ya wajib paham.

R : Kalau misalnya untuk proses *scoring* di risiko fraud itu bagaimana Pak prosesnya?

I : Oke, kalau proses *scoring* itu kita mengikuti ketentuan POJK ya. Jadi, ada ketentuannya POJK, POJK SE OJK nomor 1 tahun 2019. Itu adalah *scoring* terkait dengan profil risiko bank. Nah, itu nanti mbak bisa melihat di sana itu tata cara *scoring* itu sesuai regulator. Jadi, kita nggak bisa *scoring* asal *scoring* aja. Semuanya itu telah ditetapkan oleh POJK.

R : Dalam mempersempit peluang fraud, apa langkah konkrit yang dilakukan BPR?

I : Oke, pertama kita meng-*create* parameter-parameter yang tidak bisa diakses oleh pegawai umum. Jadi, hanya pegawai-pegawai tertentu aja yang berwenang boleh masuk di sistem tersebut. Kemudian kalau ada kesalahan, sistem kita sudah men-*detect* lebih awal. Kemudian juga pengawasan melekat, baik itu secara *offline* yang misalnya target paraf, tanda tangan dan lain-lain itu semua ter-*record*. Jadi, pengawasan melekatnya itu terinventarisir dengan baik. Nah, itu yang membuat, seharusnya membuat orang-orang ketika melakukan *fraud* itu sulit untuk melakukan. Jadi, kita membuat sistem struktur organisasi yang *flow*-nya itu

lengkap untuk meminimalisir potensi-potensi teman-teman melakukan kecurangan.

R : Kalau untuk di *Management Risk* sendiri, apakah sering dilakukan rotasi pegawai, Pak?

I : Kalau sering mungkin tidak juga, ya mungkin 3 tahun, 4 tahun. Saya sendiri 5 tahun di sana belum pindah ya. Tapi, bos saya sudah 2 kali pindah. Kemudian juga ada tim baru lagi. Jadi, saya rasa mungkin belum ya. Maksudnya belum-belum ada rotasi yang setiap tahun harus rotasi. Karena memang *Management Risk* tidak boleh terlalu banyak rotasi. Kenapa? Karena itu harus orang yang punya integritas yang baik, pemahaman perbankan yang baik, kemudian struktur dan cara berpikir yang baik.

Appendix 3. Interview Transcript 2

Interviewee : Mrs. Dian Chandra Dewi

Interview Date : 9 December 2025

Position : Legal Compliance, and APU PPT Staff

R : Researcher

I : Interviewee/Informant

R : Sejauh mana digitalisasi diimplementasikan di PT BPR Bank Sleman baik di operasional dan pengendalian internal?

I : Kalau aplikasi operasional ada ya, kita mengembangkan sendiri memang untuk aplikasi operasional. Itu transaksi operasional ya? Itu pasti ada ya, kalau aplikasi operasional kita memang mengembangkan sendiri sesuai kebutuhan kita. Untuk kemudahan kita misalkan sekarang untuk transaksi yang misalkan untuk transaksi penggajian gitu ya, kita kan mengembangkan dengan sistem itu gimana bisa langsung mentransaksikan gaji ke misalkan semua PNS gitu ya kan, semua P3K kan kita, P3K lewat kita penggajian ya, itu kita pengembangan sendiri bagaimana bisa dari sistem itu untuk melakukan upload transaksi, jadi transaksi dilakukan langsung bersamaan, berapa ribu transaksi seperti itu untuk penggajian, itu kita pengembangan sendiri.

R : Apakah nasabah bisa bertransaksi secara daring?

I : Kalau nasabah bisa bertransaksi secara daring, kalau dari dengan menggunakan *mobile banking* memang kita belum bisa ya, atau *internet banking* memang belum

bisa, tapi untuk menggunakan ATM sudah bisa, kemudian ada *virtual account* juga, mereka untuk transaksi masuk itu bisa atau bisa juga transfer lewat mobile banking dari bank lain ke Bank Sleman itu juga bisa.

R : Sejak kapan sistem tersebut diadopsi di PT BPR Bank Sleman?

I : Sebenarnya kalau untuk aplikasi operasional itu udah lama ya, udah ada sejak 5 tahun yang lalu, 10 tahun yang lalu, nah kalau untuk ATM dan *virtual account* itu memang kita mulai dari, kalau ATM itu sebenarnya udah lama dari 2020 kita udah ada, cuma untuk yang sekarang yang benar-benar bisa dipakai di banyak jaringan ATM itu baru kemarin, itu di 2022 kalau nggak salah, mungkin bisa di-*search*.

R : Apakah ada sistem atau aplikasi digital yang mendukung proses pencegahan, deteksi, atau pelaporan *fraud*?

I : Nah untuk *fraud* sendiri kalau untuk aplikasi digital ini terkait dengan transaksi ATM dan *virtual account* itu kita memang ada yang namanya sistemnya *Fraud Detection System*, FDS ya, terus dia nempel di aplikasinya itu, disitu kita buat parameternya apa sih yang kira-kira terkait *fraud* itu, misal dia transaksinya di ATM yang jangkauannya jauh dari Bank Sleman, kemudian transaksinya dua kali, di ATM yang berbeda dengan jarak yang jauh, itu kan bisa menjadi parameter terjadinya *fraud* kayak gitu, nah itu nanti akan masuk ke FDS, jadi di FDS itu nanti otomatis akan terblokir rekeningnya, nah baru setelah itu akan dilakukan cek dari bagian *fraudnya*, Anti *Fraud*, nanti akan dicek bahwa ini transaksinya apakah memang nasabah atau bukan, kalau memang bukan nasabah, nanti akan konsultasi juga sama nasabah apakah memang ini transaksi nasabah atau bukan, kalau memang itu transaksi nasabah, maka nasabah nanti bisa kesini dan bisa melakukan

penggantian ATM, soalnya mungkin ATMnya itu kalau masuk ke *red flag* itu ya, ini tuh apakah kalau memang nasabahnya dia nanti bisa ganti ATM atau dia bisa buka blokirnya, tapi kalau misalkan itu bukan nasabah, ya dia harus langsung ganti ATMnya, karena mungkin sudah terkena orang, ter-*hack* gitu ya.

R : Bagaimana digitalisasi ini mempengaruhi cara divisi Bapak/Ibu bekerja dalam mengelola risiko *fraud*?

I : Pasti iya ya, karena digitalisasi itu memang kita dalam menanggapi kebijakan *fraud*, kebijakan produk, itu kita selalu melihat risiko *fraud*nya itu juga, sehingga kebijakannya kita sesuaikan dengan kemungkinan *fraud* tersebut, kemudian kalau digitalisasi kan sekarang juga sudah banyak yang kejahatan *cyber* ya, kayak menggunakan AI, kemudian nanti bisa pakai *link-link* itu. Nah itu kita juga harus memastikan itu di sistem itu tidak bisa menggunakan hal-hal seperti itu. Cuma kan yang namanya digitalisasi semuanya berkembang ya, mungkin sekarang yang lagi *viral* kayak *link-link* itu sudah kita bisa tanggulangi, tapi kan nanti dia berkembang lagi. Jadi itu sistem itu harus dilakukan pembaruan setiap tahun untuk mengikuti pengembangan perkembangan yang kejahatan *cyber* itu apa, cuma memang pasti ada kejahatannya dulu baru kita mencari solusinya, soalnya kan memang berkembang yang dari sana.

R : Bagaimana koordinasi tugas antara Kepatuhan dengan *Internal Audit*?

I : Jadi *Internal Audit* itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi

ulang, *refreshment*. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan *Internal Audit* gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke *Internal Audit* supaya memang yang berhak untuk melakukan audit itu kan dari *Internal Audit*, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi.

R : Apakah Kepatuhan ikut bertanggung jawab dalam penerapan strategi anti *fraud*?

I : Iya pasti ya, karena kita Kepatuhan jadi kita memastikan adanya kebijakannya, kemudian kita pastikan juga ini sosialisasinya sudah dilakukan atau belum, kemudian apakah teman-teman itu memahami dari ketentuan anti *fraud* ini.

R : Berarti untuk sosialisasi itu tanggung jawabnya dari divisi Ibu, ya?

I : Iya, kalau sosialisasi untuk ketentuan *internal fraud* iya, tapi biasanya kita itu ada Tim Anti *Fraud*, disitu ada bagian Kepatuhan, kemudian ada bagian Manajemen Risiko, kemudian ada SDM, ada *Internal Audit*. Kita untuk melakukan

sosialisasi itu memang bersama-sama ya untuk temanya, tapi untuk dalam penyampaian kebijakannya itu memang dari kepatuhan.

R : Dalam me-review peraturan, apakah ada koordinasi dengan *Internal Audit*? Bagaimana?

I : Untuk *review* peraturan kalau yang terkait *fraud* itu jika memang koordinasi sama *Internal Audit* kayak tadi, jadi dari hasil temuannya itu apa, nanti kita lihat kebutuhannya, kebutuhannya apakah kebijakannya itu perlu di-*review*, atau perlu di-*refreshment* lagi, atau perlu dirubah, seperti itu.

R : Bagaimana unit Kepatuhan memastikan bahwa seluruh karyawan memahami SOP anti fraud terbaru?

I : Kita bisa melihatnya memang dari ada tidaknya *fraud* ya di tahun itu. Nah, cuma kita juga ada, ketika sosialisasi itu kita kasih *post-test*, jadi di *post-test* itu kita menentukan nilainya dia lulus berapa, nah ketika semuanya lulus maka itu sudah jadi salah satu indikator kalau SOPnya itu sudah tersosialisasi.

R : Bagaimana unit Kepatuhan memastikan bahwa seluruh elemen strategi anti fraud berjalan sesuai ketentuan POJK dan SEOJK?

I : Memang kita memastikan dulu ketentuan kita dulu ya, pas dalam kita membuat kebijakan anti *fraud* itu, kita lihat apakah sesuai POJK, SEOJK itu. Nah nanti untuk pelaksanaannya apakah sudah sesuai POJK atau belum, itu ketika ketentuan kita kan sudah tersesuaikan dengan kewajiban POJK tadi, nah jadi seperti tadi, kalau memang dari SOP kita sudah sesuai nanti kita punya pelaksanaan yang kita sosialisasi lagi, kita ukur dari ada tidaknya *fraud* di tahun itu, kemudian ada *post-test*.

R : Apa bentuk pengawasan kepatuhan berbasis sistem yang dilakukan setiap bulan/kuartal?

I : Nah, ini kalau kita juga melakukan pengawasan itu dari banyaknya pertanyaan. Jadi kita karena Kepatuhan itu juga mempunyai tugas memberikan konsultasi ke unit kerja, jadi ketika unit kerja itu berkonsultasi ke kita, kita itu akan mencatat. Jadi nanti dari pertanyaan itu kita lihat berapa banyak sih pertanyaan yang sama yang dilontarkan dari unit-unit kerja itu, berapa kali, misalnya pertanyaannya tentang poin ketentuan itu sudah ada 5 pertanyaan, dan itu sama semua, berarti mungkin dia butuh dilakukan *refreshment*. Atau mungkin ada pertanyaan-pertanyaan yang memang membutuhkan *review* kebijakan, ternyata pada pelaksanaan yang tidak bisa, nah itu kita lakukan *review* kebijakan. Terus di Kepatuhan juga kita sebenarnya melakukan analisa transaksi, ini untuk APU-PPT, itu untuk anti pencucian uang itu bisa dijadikan *fraud* juga ya sebenarnya, *fraud* dari pihak eksternal gitu, nah kita juga melakukan analisa transaksi itu pakai sistem setiap bulan.

R : Apakah ada kriteria untuk menentukan unit kerja yang akan diaudit?

I : Yang melakukan audit itu kan memang dari *Internal Audit* ya, kalau unit kerjanya itu ditentukan memang semua unit kerja itu memang diaudit, nah cuma nanti kan di pas pelaksanaan auditnya itu *on the spot* saja. Nah itu semua unit kerja itu sudah ditetapkan pas di awal tahun itu sudah ada rencana auditnya, jadi sudah ditetapkan nanti audit ini kapan. Tapi ada juga kalau misalkan terjadi *fraud*, nah itu langsung dilakukan audit seketika.

R : Kalau dari SDM di Kepatuhan sendiri, apakah sering diadakan pelatihan?

I : Ya, jadi untuk yang terkait *fraud* sendiri itu setiap tahun wajib dari POJK, jadi kita memang juga dari SDM kita sendiri itu harus mendapatkan pelatihan *fraud*. Kemudian kita juga harus melakukan pelatihan untuk kepatuhan, karena memang semua pegawai itu harus paham, jadi setiap tahun diulang gitu.

R : Apakah ada penguatan spesifik di unit Kepatuhan terkait risiko digital?

I : Kalau risiko digital tadi, untuk yang pihak eksternal, yang *fraud* eksternal, itu memang kita sudah ada yang tadi ada FDS, kemudian itu juga sudah ada ketentuannya, parameternya sudah ditetapkan. Kemudian ada juga yang kita melakukan analisa transaksi tadi, yang kita menilai internetnya mencurigakan atau engga, itu di luar FDS ya. Kemudian ada juga untuk yang *fraud* internal, itu kita bisa melihat dari sistem itu juga, wajib terdapat *audit trail*. Jadi untuk semua yang masuk ke sistem, kita pasti ada *user* dan *password*, kita sudah melakukan juga untuk membuat ketentuan harus ada, untuk membalas sistem harus ada *audit trail*-nya, kemudian disitu harus bisa dilihat siapa yang terakhir kan mengakses, apa akses apa yang dia lakukan dan dia ubah.

R : Menurut unit Kepatuhan, risiko fraud digital terbesar muncul dari sisi mana?

I : Mungkin yang dari pihak eksternal tadi ya, itu dari pengembangan kejahatan *cyber*, ada yang bisa dari *link*, nah itu memang paling banyak itu. Kemudian ada juga sekarang banyak penipuan-penipuan yang *scamming*, nah itu juga sekarang banyak terjadi. Jadi memang kalau *fraud* digital itu yang paling banyak di transaksi

digital itu ya. Yang dari pihak eksternal kalau transaksi di internal sih kita kan semua bisa ngecek, dan karyawannya pun terbatas ya, karyawannya cuma ini. Tapi kalau yang eksternal ya bisa juga ada *fraud* digital yang dari vendor-vendor, mungkin kita kan pengembangan produk layanan digital itu kerjasama dengan vendor, mungkin nanti dari vendor-vendor itu juga bisa terjadi *fraud* yang bisa berdampak ke kita.

R : Apakah *whistleblowing system* digunakan secara aktif atau pasif?

I : Kita ada melalui portal, melalui *web* Bank Sleman itu ada, untuk yang internal maupun eksternal. Misalkan pihak eksternal mau melaporkan tentang pelanggaran internal, pelanggaran pegawai Bank Sleman, itu bisa juga di *web* tersebut. Dan kita sebenarnya sudah secara aktif melakukan itu, kalau internal itu kita juga bisa melalui sistem *whistleblowing*, atau melalui langsung ke petugas *whistleblowing* nya. Jadi bisa langsung, misalkan memang tidak mau secara tertulis, dia maunya bertemu langsung, misalkan ke petugas *whistleblowing* itu juga bisa. Petugasnya itu ada di bagian SDM.

R : Berarti untuk SDM juga masuk ke dalam Tim Anti *Fraud*?

I : Ya, karena dia ada petugas *whistleblowing*, jadi dia juga masuk.

R : Bagaimana mekanisme *whistleblowing system* dilaksanakan di PT BPR Bank Sleman sejauh ini?

I : Mekanismenya memang dari laporan itu, nanti dari SDM sebagai *whistleblowing officer* tadi, dia akan melakukan deteksi dulu, dia menginvestigasi dulu, ini memang ada buktinya atau tidak. Ketika memang ada buktinya, itu akan ditindaklanjuti melalui *Internal Audit*, jadi mungkin SDM yang menyampaikan ke

Internal Audit untuk dilakukan investigasi. Kemudian dari *Internal Audit*, nanti akan melakukan investigasi *fraud*nya itu, dan akan menyatakan hasilnya nanti ke SDM. Jadi hasilnya itu memang *fraud* atau bukan. Atau mungkin bukan *fraud* namun pelanggaran ketentuan, pelanggaran ketentuan internal, tidak ada yang dirugikan, seperti itu misalnya. Nah, nanti dari SDM menarik hasil investigasi itu, kemudian akan melakukan rapat komite SDM, jadi yang berhak menentukan sanksinya itu dari komite SDM. Nah, ini memang *fraud* atau bukan, dan kemudian sanksinya apa yang akan diberikan.

R : Apakah ada kendala tertentu dalam mengimplementasikan sistem tersebut?

I : Kendalanya itu adalah ketika ada pelaporannya, tapi tidak terdapat buktinya. Jadi SDM harus mencari dulu, ini apakah memang betul atau tidak. Nah, kemudian kalau memang tidak ada buktinya, kemudian itu cuma kayak gosip atau apa, itu kan tidak bisa ditindaklanjuti. Tapi dari kendala yang di *web* itu, itu memang juga belum sempurna ya, karena harusnya kan dia bukan satu *form* yang harus di-*download*, kemudian di-*scan*, habis itu di-*upload*, itu kan agak menyulitkan sebenarnya untuk *whistleblower* ya. Nah, itu kendalanya juga di situ, jadi kita sebenarnya mau merubah itu jadi langsung inputan, langsung masuk ke *whistleblowing officer*. Tapi memang untuk pengembangan itu harus membutuhkan waktu, jadi untuk sementara kita menggunakan itu. Cuma ya itu tadi kendalanya harus di-*print* dulu, harus diisi, harus di-*upload*, kayak gitu. Terus kendalanya itu juga ada kalau untuk, kadang kan orang takut juga ya untuk melaporkan gitu ya, mungkin kalau bawahan untuk melaporkan atasannya kayak

gitu kan, walaupun sebenarnya aman, kita sudah mensosialisasikan juga, tapi kadang memang masih ada takut di-*blacklist*, kadang-kadang itu jadi juga kendala *whistleblowing*, walaupun sebenarnya sudah tanpa nama seperti itu, cuman ya itu juga masih menjadi kendala, jadi kayak angkanya *whistleblowing* itu masih rendah.

R : Apakah sering diadakan *surveillance system*?

I : *Surveillance system* itu sebenarnya kita lakukan juga, nah itu kalau kewenangannya dari IT, kalau kita juga melakukan itu, sebenarnya setahun sekali ya kita lakukan.

R : Bagaimana ketentuan perlindungan whistleblower dijamin?

I : Tentang perlindungannya, ya tadi perlindungan dari identitas menjadi rahasia, identitas *whistleblower*. Kemudian apabila masuk ke pengadilan, nah itu nanti akan diberikan fasilitas sesuai, kayak fasilitas konsultan hukum seperti itu, untuk melindungi. Kemudian untuk memberikan keterangan tanpa harus bertatap muka dengan pelaku, di setiap tingkat pemeriksaan. Kemudian perlindungannya tertinggal balasan oleh pelaku pelanggaran, yang di internal ya, yang tadi di-*blacklist*, kemudian ada tekanan, pemecatan, penggugatan hukum. Untuk ancaman, misalkan ada juga ancaman dari luar, yaitu kita juga bisa melindungi tergantung, *whistleblower*-nya itu melaporkan ancaman apa yang dia terima.

R : Bagaimana penyusunan dan pemutakhiran SOP anti fraud dilakukan dalam menghadapi risiko digital?

I : Nah itu tadi seperti, kita kan setiap tahun akan melakukan *penetration test*. Kemudian kita juga lihat apa kejahatan-kejahatan yang ada. Kemudian kalau soal internal juga, kita lihat dalam satu tahun itu, apa sih temuan dari *Internal Audit*

yang terkait dengan *fraud*, atau ada tidaknya *fraud*. Nah, ketika memang ada, kita bisa melihat kenapa bisa terjadi *fraud* itu, kekurangannya di ketentuan internal apa, jadi setiap tahun kita melakukan evaluasi tentang *fraud*.

R : Kalau dari BPR Bank Sleman ini sendiri, apakah sudah ada upaya untuk menambah kesadaran terkait *fraud*?

I : Upaya kesadaran terkait *fraud*, kita kan setiap bulan melakukan sosialisasi anti *fraud*, ke semua yang kerja, kita *rolling* setiap bulan. Kemudian juga di *desktop*-nya PC karyawan masing-masing, itu sudah kita tampilkan *wallpaper*-nya itu adalah anti *fraud*, misalkan jangan lakukan *fraud*, terus keluarga di rumah menunggu, kaya gitu. Kemudian kita juga di depan itu kan ada TV, di semua kantor cabang juga ada TV, di depan akses itu juga ada, kita juga buat dan tampilkan poster anti *fraud*. Kemudian kita juga kan di sosialisasi anti *fraud* itu, kita juga mau memberikan contoh-contoh *fraud* yang mungkin yang kita alami, jadi kasus-kasus *fraud* yang kita lihat proses hukumnya, itu kita juga sampaikan.

R : Kalau menurut Ibu sendiri, kira-kira area apa yang paling mendesak untuk diperbaiki dalam penguatan kapabilitas SDM untuk anti *fraud* itu sendiri?

I : Kalau anti *fraud*, menurut saya yang paling rentan itu bagian yang memegang uang, kayak *funding*, *lending*, kredit, kemudian bagian *teller*. Bukan Cuma di Bank Sleman namun di bank lainpun juga memang di bagian itulah yang rentan terjadi *fraud*. Karena memang setiap hari berurusan dengan nasabah, sudah tahu karakteristik nasabah, jadi setiap hari tanggung jawabnya memang mengelola dana nasabah. Jadi yang bagian yang paling rentan itu adalah itu, dan kita

tanggulanginya dengan memang kita di bagian-bagian itu kita sudah buat sistemnya. Misalkan dia mau *backup* dana nasabah, dia harus mencatat dulu, kemudian dia harus izin dulu ke atasannya, mau apa nasabah mana aja *backup*-nya, kemudian setelah selesai nanti nominalnya berapa yang dia ambil. Kemudian ketika dia akan melakukan di *teller* untuk transaksi, itu *teller*-nya juga melakukan konfirmasi, benar atau tidak, mau melakukan penarikan sebesar ini, atau benar atau tidak, buat transaksi setoran nominalnya sekian melalui akun ini. Untuk transaksi *teller* juga, mereka untuk transaksi nominal tertentu, mungkin kalau di kita itu sekitar 15 juta, itu harus ada *approve* dari atasannya, mau dia penarikan atau setoran, kemudian ada juga untuk rekeningnya, yang sudah lama tidak bertransaksi, kadang ada rekening yang memang nasabah menabung satu miliar misalnya, dan itu memang dia mau disimpan buat investasi, jadi nggak pernah ditarik atau apa, itu kan kita juga ada sistemnya langsung sebagai rekening pasif, jadi dia tidak bisa melakukan transaksi, memang nasabahnya sendiri yang melakukan transaksi, itu harus butuh *approve* dari atasannya.

R : Apakah ada rekomendasi yang kira-kira perlu dilakukan PT BPR Bank Sleman untuk memperkuat pencegahan dan deteksi *fraud*?

I : Sebenarnya sudah banyak yang kita lakukan, cuma kan memang tidak sempurna gitu ya. Karena memang dari sistem pun, kalau bukan dari individunya sendiri, yang memang membatasi untuk melakukan *fraud* itu, itu akan sulit gitu. Karena kayak sistem tadi lakukan sistem ini, itu tetap bisa, lama-lama dia akan tahu, oh nanti ada konfirmasi, lama-lama dia akan pasti tahu celahnya ya. Jadi kalau sistem pun sebenarnya masih ada ruang gitu, jadi harus kita kemampuan perbaikan setiap

tahun. Dan kalau ada terjadi *fraud* tadi, kita bisa lihat, oh kenapa ini bisa terjadi *fraud*, kekurangan kita apa. Mungkin memang sosialisasi ya, misalkan *fraud* yang memang terjadi dekat gitu, jadi memang di karyawan sendiri tumbuh, karyawan tidak ada niat untuk melakukan *fraud*, dan dia jadi sadar bahwa, oh nanti kalau aku *fraud*, aku bisa dipenjara, aku bisa di-*blacklist*. Memang sistem baik ya, memang bisa menghalau, tapi memang dari orangnya sendiri, jadi kita harus meningkatkan kesadaran *fraud*, kita juga ada setiap bulan itu ada pengajian, mungkin biar kalau mereka, kalau kaya gitu tuh dosa, dari sisi keyakinannya.

R : Apakah ada rekomendasi kegiatan yang bisa Ibu ajukan atau dari unit Kepatuhan sendiri, dalam rangka meningkatkan kualitas SDM?

I : Kalau pelatihan kan memang, kita terus ya, kita sosialisasikan, kemudian kita juga kasih contoh-contoh, mungkin sebenarnya yang paling, apa ya, mengena itu ya kayak contoh-contoh itu, ya. Atau mungkin kalau ada terjadi *fraud* internal di Bank Sleman gitu kita bisa sampaikan dampaknya seperti apa agar lebih mengena gitu. Karena *real* terjadi dan kita bisa lihat sendiri sekarang orangnya seperti apa keadaannya. Atau kita juga bisa *sharing* dengan bank-bank lain, kan itu banyak ya yang ada di internet, kita bisa ambil itu.

Appendix 4. Interview Transcript 3

Interviewee : Mr. Arif Setiawan

Interview Date : 9 December 2025

Position : Senior Internal Audit

R : Researcher

I : Interviewee/Informant

R : Kalau untuk di *Internal Audit* sendiri, apakah terlibat di program *anti-fraud awareness* di BPR Sleman dan juga bagaimana implementasinya di lapangan?

I : Jadi kalau dari *Internal Audit* kita kan juga masuk di tim SAF (Tim Strategi Anti *Fraud*) ya. Jadi kita bareng misalnya dari unit-unit kerja itu kan juga sudah menjalankan, kemudian dari Satuan Kepatuhan, Manajemen Risiko, juga kita dari *Internal Audit* itu kan kita lebih ke istilahnya setelah misalnya ada kejadian, biasanya seperti itu. Jadi kalau misalnya ada indikasi *fraud* ini kita biasanya nunggu tugas dari dirut, kalau misalnya ada penugasan baru kita terima seperti itu.

R : Kalau misalnya proses identifikasi kerawanan *fraud* sendiri itu bagaimana, Pak?

I : Kalau *fraud* kita biasanya kalau dari audit itu lebih ke ini ya, kita kan biasanya ada pengawasan, jadi ada pengawasan itu istilahnya kita mengadakan pemeriksaan, jadi sampai bagaimana SOP-nya dijalankan. Kemudian ada misalnya deteksi, misalnya kita melakukan investigasi juga, misalnya dari proses ada pola-pola yang

tidak sesuai seperti itu. Kita juga konsultatif, jadi misalnya dari pelaksanaan dari masing-masing unit kerja itu ada hal-hal yang rentan atau apa, biasanya kita memberikan rekomendasi seperti itu, biar lebih bagus atau lebih kuat, *fraud awareness*-nya.

R : Untuk mekanisme pemeriksaan dari *Internal Audit* sendiri untuk menerapkan strategi anti *fraud* itu bagaimana, Pak?

I : Kalau yang biasanya kita lakukan sebenarnya kan untuk audit kan memang tujuannya juga sebagian besar untuk deteksi *fraud* ya, jadi kalau kita memang awal kan kita harus merencanakan. Jadi untuk membuat perencanaan itu, kita kalau sekarang itu biasanya untuk memeriksa itu berdasar dari tingkat risiko, sebenarnya tingkat risiko *fraud* atau yang kemungkinan hal-hal yang rentan terjadi penyalahgunaan atau penyelewengan itu kita buat untuk ininya, untuk perencanaannya. Nanti setelah perencanaan kita juga harus tahu ruang lingkupnya, nanti objeknya atau fokusnya yang harus kita periksa itu apa saja, seperti itu. Lalu nanti untuk pelaksanaannya setelah nanti kita pelaksanaan untuk pemeriksaan, yang kita tahu ya mungkin nanti kita ada evaluasi juga, mungkin ada penyimpangan atau tidak kesesuaian, kita biasanya memberikan rekomendasi atau tindak lanjut. Nanti setelah dari unit itu melakukan tindak lanjutnya ya kita juga cek lagi, sampai sejauh mana dilaksanakan dari tindak lanjut dari rekomendasi dari audit.

R : Apakah sering dilakukan *surprise audit*, Pak?

I : Kalau yang penting kita setiap bulan pasti minimal ada satu kali kas opname ya, jadi terutama untuk kas besar, di brankas itu ya kita berusaha untuk itu, *surprise*

audit kita cek, kemudian juga kaitannya inventaris seperti tabungan, materai, dan lain-lain itu juga kita cek, minimal itu sih.

R : Berarti rutin sebulan sekali ya, Pak?

I : Iya, cuman ya memang kita berusaha untuk kapan atau waktunya itu ya acak lah, soalnya kan ya kaitannya kan memang kas, nominal.

R : Apakah hanya dilakukan di kantor pusat atau ada kemungkinan di kantor cabang juga, Pak?

I : Di semua, di semua kantor cabang juga kita periksa, misalkan kebetulan kalau pas jadwalnya untuk kerja misalnya kita periksa cabang, itu ya di kantor kas juga kita ajak, jadi kita *on the spot* ke sana.

R : Apakah ada indikator untuk melakukan *surprise audit*, untuk menentukan kantor mana yang diperiksa?

I : Setiap bulan kita periksa semuanya.

R : Berarti tidak ada indikator tertentu ya, Pak?

I : Ya, istilahnya untuk penjagaan awalan juga kita setiap bulan, soalnya kan ya apa ya, itu tadi untuk kita perbankkan kan, ini ya utama kan kas ya, jadi istilahnya itu untuk pemeriksaannya lebih.

R : Kalau terindikasi munculnya dugaan *fraud*, apakah *Internal Audit* langsung turun tangan menindaklanjuti atau bagaimana mekanismenya, Pak?

I : Kalau kita kan di awalkan, kalau ada indikasi kan dari *whistleblower*, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja,

kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, *role input*-nya, kemudian *timeline*-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa.

R : Dalam mekanisme tersebut apakah dilakukan juga *surveillance system*?

I : Lebih ke IT ya, istilahnya kan kalau untuk transaksi memang kita pasti juga ngecek, untuk di SKAI itu ada yang *basic*-nya IT juga, jadi untuk transaksi-transaksi kita ada *log user* dan sebagainya itu tetap kita cek juga. Tapi misalnya ada pola-pola yang istilahnya, ya tidak normal lah istilahnya dan kita sudah dicek di sistem juga.

R : Apa saja yang dilakukan untuk menjaga kredibilitas dalam melaksanakan tugas dari *Internal Audit* sendiri, Pak?

I : Untuk menjaga independensi kan kita tidak boleh terlibat di operasional langsung, jadi kebetulan kalau di bagian lain, dulu saya masih di analis itu bisa jadi tim pengadaan dan sebagainya, tapi kalau kita sudah di Audit Internal, kita tidak bisa terlibat untuk menjaga independensi. Kalaupun mau memeriksa pun, misalnya saya dari bagian analis, saya mau memeriksa bagian yang saya sebelumnya, kita

juga sesuai ketentuannya, di OJK pun harus ada minimanya beberapa bulan baru bisa masuk periksa.

R : Kalau dalam konteks digital, kira-kira dalam mekanisme audit sendiri apakah ada perubahan yang menyesuaikan digitalisasi, Pak?

I : Memang kan kita tetap harus menyesuaikan, itu pun juga selain kita dari internal untuk pemeriksaan misalnya IT, kita pun juga ada pemeriksaan dari eksternal, yaitu biasanya 3 tahun sekali apa ya, jadi kita juga ada, kita tetap diaudit juga dari eksternal, kaitannya dengan IT. Dan untuk auditnya sendiri, bagian Audit Internal kita, itu juga nanti juga ada dari eksternal, sampai sejauh mana kita pelaksanaannya.

R : Terkait anti *fraud*, apakah sering dilakukan pelatihan, baik untuk *Internal Audit* sendiri ataupun untuk seluruh pegawai?

I : Untuk seluruh pegawai kita sudah ada ketentuannya, jadi minimal satu kali untuk seluruh pegawai itu ada pelatihan tentang SAF, sekarang wajib itu SAF, selain ada APU-PPT dan sekarang ada yang konsumen, perlindungan konsumen itu juga sama. Jadi itu sudah ada ketentuan kalau satu kali harus wajib seperti perlindungan konsumen. Dan kalau untuk *Internal Audit* sendiri, kita setiap ada hal-hal baru, kaitannya dengan audit, kita dapat ketentuan baru, biasanya kita juga nanti kita mengikuti untuk pelatihannya, yaitu nanti yang diadakan dari kantor sendiri, atau mungkin dari luar kita ngirim peserta ke sana.

R : Apakah pelatihannya efektif terhadap kinerja SDM *Internal Fraud*, Pak?

I : Sejauh ini sangat membantu, jadi kita pun *alhamdulillah* untuk tim SKAI Bank Sleman, itu kita tiga orang, jadi ada kepala SKAI, kemudian *staff*-nya dua. Itu

kebanyakan sudah kita ikutkan untuk sertifikasi juga, sertifikasi khusus untuk PE, jadi Pejabat Eksekutif Audit Internal. Istilahnya kita sudah ada kompetensi juga.

R : Kalau untuk ditempatkan di *Internal Audit* sendiri, apakah ada kriteria SDM yang harus dicukupi, Pak?

I : Kalau untuk kriterianya, yang pertama integritas dan independensi, kemudian kita punya kemampuan analisa seperti itu, yang kaitannya dengan audit.

R : Menurut Bapak, apakah mekanisme yang diterapkan saat ini di BPR Bank Sleman sudah cukup untuk meminimalkan *fraud* yang terjadi?

I : Untuk mekanisme sekarang, kemudian juga untuk *fraud*, kemudian kita sudah membentuk tim, kita juga berusaha untuk melengkapi instrumen yang diperlukan, seperti ada SOP dengan pelaksanaan di unit-unit kerja. Kemudian ada ketentuan-ketentuan mungkin dari Satuan Kerja Kepatuhan (SKK) yang harus dipatuhi, pun dari tim Manajemen Risiko juga sudah rutin untuk memitigasi keadaan risiko-risiko, atau peluang-peluang yang bisa membuka celah ke depannya *fraud*. Itu *insya Allah* untuk Bank Sleman sudah cukup bagus menurut saya.

R : Apakah ada kendala yang mendesak untuk diperbaiki di divisi Bapak sendiri?

I : Untuk Audit Internal ya? Kalau Audit Internal, kita berusaha untuk *update* terus ya, *update* info. Kemudian kita juga harus meningkatkan kompetensi, kaitannya dengan hal-hal yang baru, misalnya ada kemarin, apalagi sekarang IT ya, misalnya IT ya, paling nggak, gak harus jurusan IT, paling nggak kita juga harus mampu, bisa mengetahui, misalnya yang dasar-dasar untuk istilahnya pemeriksaan.

R : Kalau dari Bank Sleman sendiri, upaya apa yang sering dilakukan untuk menambah kesadaran terkait *fraud*?

I : Kita harus senantiasa mendorong semua karyawan ya, misalnya semua yang ada di sini untuk budaya anti *fraud*. Paling nggak ada berapa TV, itu kan setiap hari menampilkan *zero fraud*. Kemudian juga dari masing-masing unit kerja, juga ada sosialisasi. Kemudian dari Tim Anti *Fraud* sendiri itu ada rutin, jadi kita sosialisasi, *share refreshment*, kaitannya dengan anti *fraud*.

R : Apakah ada rekomendasi dari Bapak untuk meningkatkan kapabilitas SDM di divisi *Internal Audit*?

I : Ya, mungkin untuk pelatihan, kalau bisa untuk peningkatan kompetensi kan, tidak harus yang massal ya. Paling nggak kan *refreshment* atau *group discussion* yang bisa rutin, paling nggak berapa orang, jadi mungkin bisa lebih mendalam, lebih tersampaikan seperti itu.

R : Untuk pelatihan yang dilakukan selama ini, biasanya bentuknya studi kasus atau teori, Pak?

I : Dua-duanya, tapi biasanya lebih banyak langsung studi kasus ya, kayak aku dulu belajar juga kan, kita bisa lebih paham kalau ada langsung contoh implementasinya, jadi ya sudah tahu kok, bedanya seperti ini, teori seperti ini, jadi bisa lebih memahami.

R : Dari sistem digital sendiri, apakah ada gap atau keterbatasan sistem yang dirasakan dalam upaya meminimalkan *fraud*, Pak?

I : Kalau untuk IT ya *alhamdulillah* terus berkembang, ada *reading* juga istilahnya, terus pengembangan, katanya dengan vendor pun juga komunikasi juga bagus. Jadi

misalnya ada hal-hal yang mungkin perlu atau masih ada celah ya, kita komunikasikan. Jadi antara ini sih, antara mereka, dari audit kan kita juga memberikan masukan.

R : Di *Internal Audit* sendiri, apakah ada sistem yang mendukung proses pendeteksian *fraud*?

I : Sistem khusus, enggak ada, belum ada ya, kita lebih ke ini sih, kalau untuk analisa kan, kita melihat pola-pola transaksi, kemudian dokumen seperti itu. Kalau sistem khusus, belum ada, misalnya aplikasi, kalau secara sistem ini kan ya itu tadi, kita melihat pola-pola dan yang dihitungin kerja yang terjadi di sana, mungkin ada penyimpanan yang tidak biasa, tidak normal, bisa jadi indikasi.

R : Tadi disebutkan sudah ada jadwal audit yang setiap bulan gitu ya Pak, lalu untuk pembagian jadwalnya dengan *surprise audit* itu bagaimana Pak?

I : Jadi kalau yang terjadi di Bank Sleman, kita kan sudah membuat rencana untuk satu tahun ya, itu kan sudah untuk pemeriksaan khusus unit-unit kerja. Tapi kalau untuk yang kas opname, itu sudah rutin, jadi selain kita yang audit tentang kerja dengan unit-unit kerja itu, tetap yang kas opname kita jalankan setiap bulan, jadi bareng istilahnya itu.

R : Untuk di *Internal Audit* tadi disebutkan bahwa setelah ada indikasi *fraud*, *Internal Audit* yang menginvestigasi sampai ada laporannya, kalau untuk tindak lanjut ke pelakunya itu bagaimana Pak?

I : Kalau dari *Internal Audit* kita cuma merekomendasikan, jadi untuk sanksi, kita ya sesuai, kita rekomendasikan sesuai dengan peraturan perusahaan. Kalau untuk

keputusan, kita sudah ada, yang terkait dengan SDM, sudah urusan SDM sendiri, jadi yang kita serahkan dulu dengan komisaris.

R : Bagaimana mekanisme terkait pengumpulan bukti, Pak?

I : Tadi kalau untuk pengumpulan bukti kan kita bisa dari dokumen, kemudian dari *on the spot*, kemudian wawancara langsung bisa, kemudian dari transaksi, misalnya dari *vouching* seperti itu.

R : Alat untuk sistem pengawasan dan keamanan sendiri ada apa saja ya, Pak?

I : Pengawasan? Ya, kita pakai ini, sesuai SOP dan *job desc*, kita sesuaikan. Jadi khusus unit kerja kan pasti ada, setiap bagian ada *job desc*. Kemudian untuk melaksanakan sesuatu itu ada SOP, ini kita sesuaikan, apakah sudah sesuai dengan ketentuan, kepatuhan tersebut. Biasanya kalau tidak sesuai, ini kan ada peluang, ada peluang yang kemungkinan nanti bisa menimbulkan *fraud*.

R : Untuk pelatihan sendiri di *Internal Audit* itu biasanya materinya mencakup apa saja ya, Pak?

I : Untuk *Internal Audit*, yang saya ikuti itu banyak ada audit investigatif, kemudian, misalnya kaitannya dengan audit IT, biasanya lebih ke ini sih, apa ya, yang isu-isu baru juga sih ketentuan-ketentuan baru, seperti itu, saya baru setahun juga. Kemarin ikutnya juga investigatif, kemudian juga, istilahnya itu tadi sertifikasi kan lebih umum ya, ada perundang-undangan, kemudian juga tata kelola dan audit internalnya sendiri.

R : Kalau di *Internal Audit* apakah sering ada *turnover* pegawai, Pak?

I : Agak lama sih, sesuai kebutuhan sih, jadi kalau memang ada rotasi atau apa, ya kemungkinan, tapi kalau yang kemarin, ya itu agak lumayan lama.

Appendix 5. Interview Transcript 4

Interviewee : Mrs. Rizky Chitra
 Interview Date : 10 December 2025
 Position : Human Capital Staff

R : Researcher

I : Interviewee/Informant

R : Menurut Bapak/Ibu, kompetensi apa saja yang wajib dimiliki anggota Tim Anti *Fraud* di era digital?

I : Kompetensi kemampuan *analytic thinking*, kemampuan komunikasi yang baik, dan juga pendalaman pemahaman terkait hukum.

R : Bagaimana proses *screening*, *Know Your Employee* internal, dan rekrutmen dilakukan untuk memastikan integritas pegawai?

I : Pada saat proses seleksi, tim SDM melakukan *screening* melalui media sosial dan SLIK BI, selain itu tim SDM melakukan verifikasi dengan perusahaan sebelumnya, apabila pernah bekerja sebelumnya, atau verifikasi dengan pihak yang mereferensikan.

R : Bagaimana proses *Know Your Employee* internal dilakukan?

I : Untuk pegawai yang sudah masuk, tim SDM melakukan pemeriksaan SLIK BI secara berkala dan pemantauan media sosial maupun gaya hidup selama di kantor.

R : Apakah terdapat pelatihan khusus terkait *fraud* digital, *cyber fraud*, *forensic audit*, atau penggunaan sistem digital audit?

I : Untuk saat ini belum ada, yang diwajibkan saat ini adalah pelatihan strategi anti *fraud* bagi seluruh pegawai. Tim Anti *Fraud* secara berkala melakukan sosialisasi terkait SAF.

R : Apakah ada culture audit untuk menilai budaya integritas pegawai?

I : Belum ada.

R : Apakah pelatihan diadakan dengan bekerja sama dengan pihak pemerintahan atau swasta? Dan seberapa rutin pelatihan dilakukan?

I : Pelatihan SAF dilakukan sekali setiap tahun oleh narasumber, baik perorangan atau instansi swasta. Sosialisasi SAF dilakukan secara berkala oleh tim SAF.

R : Bagaimana mekanisme evaluasinya?

I : Mekanisme evaluasi berupa kuis setelah dilakukan sosialisasi oleh tim SAF tadi.

R : Apakah pelatihan digital *fraud* sudah adaptif atau masih bersifat umum?

I : Untuk pelatihan digital *fraud* saat ini belum pernah dilaksanakan.

R : Apakah ada gap kompetensi yang dirasakan? Jika ada, gap apa yang paling signifikan?

I : Tidak terdapat gap kompetensi yang terlalu lebar. Gap kompetensi yang terasa di beberapa bagian kemungkinan dikarenakan perbedaan usia sehingga pola pikir dan pola kerja terasa berbeda.

R : Apakah ada gap generasi dalam pemahaman digital?

I : Ada gap generasi terhadap proses digitalisasi. Seperti pada umumnya, untuk pegawai dengan usia di atas 45 tahun lebih sulit beradaptasi dengan proses digitalisasi dibanding pegawai dengan usia produktif.

R : Bagaimana evaluasi kinerja bagi pegawai yang menjalankan fungsi anti *fraud* dilakukan?

I : Evaluasi kinerja dilakukan setiap semester melalui sistem KPI.

R : Apakah ada *reward* dan *punishment* atau jalur karir yang berpengaruh pada integritas pegawai?

I : Terdapat *punishment* atau demosi, PHK bagi pegawai yang melakukan tindakan-tindakan menyimpang seperti *fraud* atau penipuan dan lain-lain.

R : Rotasi pegawai dilakukan berapa tahun sekali?

I : Rotasi dilakukan 3 sampai 5 tahun sekali.

R : Bagaimana tingkat *turnover* pegawai selama beberapa tahun terakhir?

I : *Turnover* cukup rendah ya, rata-rata 1 sampai 2 pegawai per tahun, dengan jumlah pegawai 170 orang.

Appendix 6. Interview Transcript 5

Interviewee : Mrs. Rizky Chitra
 Interview Date : 22 December 2025
 Position : Human Capital Staff

R : Researcher

I : Interviewee/Informant

R : Bagaimana prosedur rekrutmen pegawai yang akan ditempatkan di *internal control*?

I : Prosedur rekrutmen sama seperti rekrutmen bagian lain. Diawali dengan seleksi dokumen lalu *interview user* lalu psikotes atau tes kemampuan dasar, *medical check up*, dan *interview* direksi.

R : Adakah program pengembangan karir untuk staf yang bertugas dalam Tim Anti *Fraud*?

I : Tidak ada program pengembangan karir yang khusus atau spesifik untuk jabatan tersebut.

R : Terkait penerapan strategi anti *fraud*, apakah terdapat SOP-nya? Jika ada, bagaimana mekanisme penerapannya dan apa kekurangannya (jika ada)?

I : Terdapat SOP terkait penerapan dan kekurangan mungkin bisa ditanyakan ke bagian kepatuhan selaku pembuat kebijakan atau *review* kebijakan.

R : Apa tantangan terbesar dalam membangun budaya anti *fraud* di BPR?

I : *Awareness* pegawai. Kesadaran akan risiko *fraud* serta kurangnya keberanian pegawai untuk melaporkan kejadian yang dicurigai sebagai tindakan *fraud*.

R : Bagaimana proses pengecekan latar belakang calon pegawai dilakukan?

I : Proses pengecekan latar belakang antara lain dengan pengecekan SLIK minimal 1 tahun sekali, pengecekan media sosial atau kunjungan ke tempat tinggal pegawai.

R : Sejauh mana efektivitasnya?

I : Sejauh ini yang paling efektif adalah pengecekan SLIK. Karena dari SLIK dapat dilihat gaya hidup pegawai dan pinjaman yang dimiliki, seperti pinjol atau *paylater* yang berisiko.

R : Apakah terdapat prosedur tertulis untuk rekrutmen pegawai?

I : Terdapat SOP tertulis terkait hal tersebut.

R : Saat melakukan proses rekrutmen, apakah dilakukan rekam jejak pegawai yang secara khusus hanya dilakukan untuk calon pegawai *Internal Audit*, MR, Kepatuhan dan SDM? Jika dilakukan, rekam jejak yang bagaimana dan apa tujuan secara khususnya?

I : Rekam jejak pegawai dilakukan untuk semua calon pegawai. Apabila calon pegawai sudah pernah bekerja, maka dilakukan pengecekan ke perusahaan lama, *cross check* dengan bagian HRD apakah calon pegawai tersebut memiliki rekam jejak yang baik atau kurang baik di perusahaan sebelumnya. Selain itu saat ini sudah ada aplikasi SIPELAKU dari OJK sehingga bagian SDM bisa mengecek apakah calon pegawai tersebut pernah terlibat dalam tindakan *fraud* sebelumnya. Tujuannya untuk menghindari penerimaan pegawai yang memiliki rekam jejak yang kurang baik.

R : Bagaimana dengan sertifikasi? Apakah calon pegawai tersebut akan lebih dipertimbangkan? Bagaimana bobotnya?

I : Sertifikasi juga termasuk dalam pertimbangan pada saat seleksi, calon pegawai yang memiliki sertifikasi yang sesuai dengan jabatan yang dilamar akan lebih dipertimbangkan. Tidak ada bobot khusus terkait sertifikasi.

R : Dari masing-masing bagian, khususnya yang di bawah Direktorat Kepatuhan dan SDM, apakah pernah mengajukan persyaratan khusus untuk pegawai yang akan ditempatkan di bagiannya?

I : Tidak ada persyaratan khusus, tetapi lebih diutamakan yang sudah memiliki pengalaman.

R : Menurut SDM, *gap* kompetensi apa yang saat ini paling krusial dalam penguatan anti *fraud* di Bank Sleman?

I : Pemahaman regulasi dan kebijakan, masih banyak pegawai yang belum memahami terkait regulasi dan kebijakan.

R : Dalam 3-5 tahun ke depan, kompetensi apa yang wajib dimiliki Tim Anti *Fraud* untuk menghadapi risiko digital?

I : Pemahaman terkait perubahan regulasi, analisis data, dan mungkin terkait penggunaan teknologi informasi.

R : Apakah Bank Sleman pernah membandingkan strategi penguatan Tim Anti *Fraud* dengan BPR lain?

I : Sejauh ini belum pernah.

R : Bagaimana perencanaan pelatihan tahunan disusun?

I : Berdasarkan risiko lalu evaluasi kinerja serta usulan dari setiap unit kerja.

R : Jenis pelatihan apa yang diimplementasikan kepada para pegawai yang bertanggung jawab atas Tim Anti *Fraud*? Apakah bersifat teori atau kasus aktual?

I : Sejauh ini untuk pelatihan masih bersifat teoritis. Karena tim anti *fraud* masih cukup baru maka saat ini masih berfokus pada teori agar pegawai lebih memahami teorinya terlebih dahulu.

R : Apa kelebihan dan kekurangannya?

I : Kelebihannya pegawai paham mengenai teori dan regulasi. Kekurangannya pegawai belum dapat terjun praktik apabila terjadi *fraud*.

R : Dalam satu tahun terakhir, berapa kali pelatihan tersebut dilakukan untuk masing-masing jenis dan materi yang termasuk ke dalam pelatihan pencegahan dan pendeteksian *fraud*?

I : Untuk tahun 2025 sudah dilakukan satu kali pelatihan untuk seluruh unit kerja dan satu kali sosialisasi internal untuk seluruh pegawai. Namun ada beberapa pegawai yang mengikuti *online training*.

R : Pihak mana yang ditunjuk oleh Bank Sleman sebagai narasumber dalam pelatihan yang tersebut?

I : Bank Sleman bekerjasama dengan lembaga swasta ataupun perorangan sebagai narasumber dalam pelatihan SAF.

R : Apa alasan pemilihan narasumber tersebut?

I : Karena yang bersangkutan telah memiliki pengalaman mengajar SAF.

R : Siapa yang mengajukan pelatihan tersebut?

I : Pelatihan tersebut sebelumnya telah diusulkan oleh penanggung jawab SAF yaitu bagian SKMR.

R : Bagaimana perubahan kinerja pegawai yang bertanggung jawab atas pencegahan dan pendeteksian *fraud* sebelum dan sesudah diberikan pelatihan?

I : Untuk perubahan belum dapat dilihat secara langsung tapi minimal pegawai sudah mengerti dan paham terkait strategi anti *fraud*.

R : Apakah ada indikator kinerja sebelum dan sesudah pelatihan?

I : Belum ada indikator kinerja sebelum dan sesudah pelatihan.

R : Faktor apa yang menyebabkan pelatihan tidak efektif?

I : Kurangnya konsentrasi peserta pada saat pelatihan, narasumber yang kurang mumpuni di bidangnya.

R : Apa saja indikator pelatihan bisa dikatakan tidak efektif?

I : Apabila tidak ada perubahan atau tidak diterapkan di unit terkait. Di Bank Sleman untuk setiap pelatihan wajib dilakukan *pre-test* dan *post-test* untuk mengukur keseriusan peserta pada saat mengikuti pelatihan.

R : Apakah Bank Sleman secara khusus memberikan pelatihan atau pembekalan keterampilan dan pengetahuan kepada para pegawai yang terkait dalam penerapan strategi anti *fraud* maupun penanganan *fraud*?

I : Untuk saat ini belum ada pelatihan khusus. Hanya saja untuk Tim Anti *Fraud* lebih sering mengikuti pelatihan baik secara *offline* atau *online* terkait SAF dibanding dengan pegawai di unit kerja lainnya.

R : Bagaimana cara Bank Sleman dalam mensosialisasikan adanya *Whistleblowing System* (WBS) kepada para pegawai secara umum? Apakah terdapat kekurangan? Jika ada, mohon dapat dijelaskan bagaimana kekurangannya.

I : Bank Sleman memiliki pedoman terkait WBS dan sudah di-*share* di portal ketentuan internal sehingga setiap pegawai dapat mengakses secara bebas. Pada saat sosialisasi di setiap unit kerja, Tim Anti *Fraud* juga menjelaskan terkait WBS. Kekurangannya pegawai masih kurang *aware* terkait WBS dan masih takut untuk mengungkap kecurangan ataupun *fraud* di unit kerjanya.

R : Apa terdapat pelatihan atau keterampilan khusus maupun pengetahuan yang dibekali oleh Bank Sleman kepada pegawai yang mengelola WBS?

I : Belum ada.

R : Bagaimana SDM memastikan pegawai tetap berani menggunakan WBS?

I : Saat ini SDM hanya bisa mengingatkan atau memberi *reminder* terkait pentingnya WBS dan meyakinkan pegawai bahwa WBS ini aman sehingga identitas pelapor tidak akan bocor dan dirahasiakan.

R : Apakah diadakan pelatihan atau pembekalan keterampilan lainnya kepada pegawai untuk menunjang kinerjanya dalam melakukan *surveillance system*? Jika ada, bentuk pelatihan atau pembekalan keterampilan dan pengetahuan yang seperti apa dan bagaimana proses, *outcome* dan kekurangannya?

I : Untuk saat ini belum ada. Tapi kedepannya untuk bagian IT ataupun bagian terkait akan dilakukan sertifikasi berkala terkait keamanan sistem dan hal lain yang berkaitan.

R : Apakah diadakan pelatihan atau pembekalan keterampilan lainnya kepada pegawai untuk menunjang kinerjanya dalam melakukan *surprise audit*? Jika ada, bentuk pelatihan atau pembekalan keterampilan dan pengetahuan yang seperti apa dan bagaimana proses, *outcome* dan kekurangannya?

I : Saat ini belum ada dan rencananya akan diberikan pelatihan di tahun 2026.

R : Bagaimana SDM membangun budaya anti *fraud* lintas generasi pegawai?

I : Saat ini untuk membangun budaya anti *fraud*, tim SAF sudah melakukan antara lain, sosialisasi di setiap bagian, penggantian *wallpaper* setiap *desktop* terkait bahaya *fraud*, pembacaan kode etik bankir pada saat *morning briefing*, pemasangan poster-poster yang berisikan *reminder* akan bahaya *fraud*, dan lain-lain.

R : Apa yang dilakukan untuk meningkatkan kesadaran anti *fraud* bagi semua pegawai?

I : Sama ya mbak seperti tadi, lalu ada penandatanganan pakta integritas juga setiap tahun.

R : Apa ada perlakuan khusus untuk meningkatkan kesadaran anti *fraud* bagi unit yang berisiko tinggi seperti *teller*, kredit, dan *funding*?

I : Kalau dari bagian SDM tidak ada perlakuan khusus, mungkin bisa ditanyakan ke bagian audit internal atau manajemen risiko.

R : Apakah hasil audit atau temuan fraud menjadi dasar evaluasi SDM untuk melakukan pelatihan lebih lanjut atau pembuatan regulasi? Bagaimana prosesnya?

I : Iya. Berdasarkan temuan *fraud*, dari tim SAF akan membahas terkait temuan tersebut dengan manajemen, evaluasi sistem. Apabila dirasa ada yang perlu diubah atau di-*update* maka tim SAF akan mengusulkan perubahan atau pembuatan regulasi serta usulan pengadaan pelatihan.

R : Apakah ada kendala dalam pelaksanaan semua pelatihan dan strategi dalam meningkatkan kesadaran anti *fraud*?

I : Tidak ada.

R : Bagaimana SDM menilai efektivitas pelatihan anti *fraud*?

I : Efektifitas selama pelatihan dapat dilihat dari nilai *pre-test* dan *post-test* peserta. Sedangkan efektifitas setelah pelatihan dapat dilihat dari jumlah *fraud* yang terjadi serta kesalahan-kesalahan dalam pelaksanaan pekerjaan.

R : Apa ada rekomendasi untuk peningkatan kualitas dan kapabilitas SDM yang menangani *fraud* dan tim anti *fraud*?

I : Untuk tim SAF sebaiknya diikutkan sertifikasi namun kendala waktu dan terbatasnya lembaga yang memiliki izin terkait sertifikasi tersebut.

Appendix 7. Interview Transcript 6

Interviewee : Mr. Dwi Handoyo Miharjo

Interview Date : 2 February 2026

Position : Risk Management Staff

R : Researcher

I : Interviewee/Informant

R : Kemarin ada arahan tambahan dari Pak Hendi terkait pelaksanaannya. Mungkin langsung mulai saja ya, Pak. Untuk potensi-potensi *fraud* yang dapat muncul di Bank Sleman sendiri dan perlu dicegah dengan penerapan strategi anti-fraud, kira-kira apa saja, Pak?

I : Baik, sebelumnya *disclaimer* dulu ya. Per tanggal 22 Januari 2026 saya mendapat amanah baru di unit kerja *lending* atau *linkage*, jadi lebih sering berurusan dengan korporat dan instansi. Namun terlepas dari itu, seluruh unit kerja memang wajib memahami risiko, apalagi saya juga sudah sekitar lima tahun berkecimpung di manajemen risiko, jadi ya saya merasa ini ya saya akan memberikan referensi ya kepada mbak. Mbak Tika oke, tadi potensi-potensi *fraud*, jelas ada beberapa hal potensi *fraud* yang kita anggap itu sebagai *inherent fraud* atau *fraud* yang lengkap. Yang pertama namanya kredit uang keluar Itu risikonya pasti ada salah satunya adalah *fraud*, dimana uang tersebut yang kita salurkan ke nasabah. Itu berpotensi dimanfaatkan oleh oknum-oknum tertentu Misalnya, oke karena pencairannya selesai mendapat gratifikasi, mendapat imbalan, mendapat

hal-hal yang diluar ketentuan perbankan atau regulasi. Kita semua sepakat kalau gratifikasi itu juga termasuk salah satu bagian dari *fraud*. Jadi hal-hal seperti itu ada potensi Mbak Tika. Kemudian yang kedua juga di unit kerja lain, ada karena kita bersinggungan langsung dengan nasabah, kita punya namanya program *delivery service*, kemudian kita punya juga program *pick up service*. Dimana kalau petugas kita itu tidak memiliki integritas yang bagus, itu akan berpotensi disalahgunakan uang yang diambil atau uang yang di-*pick up*, uang yang di-*delivery* itu bisa disalahgunakan, kemudian tidak disetorkan di bank. Itu hal-hal yang sangat memungkinkan terjadi Kemudian, ya sebenarnya banyak yang di perbankan, ya itu dua contohnya. Mungkin sekaligus saya akan membahas terkait dengan antisipasinya seperti apa. Nah, antisipasinya kita setiap tahun, bahkan baru bulan ini juga, bulan Januari 2026. Itu kami menyelenggarakan semacam penandatanganan pakta integritas. Kita ada penandatanganan pakta integritas, ada penandatanganan kode etik perbankan Ada juga deklarasi anti-fraud. Jadi ini dilakukan setiap 6 bulan sekali di perbankan kami. Nah, selain itu apalagi, selain itu kita memiliki pengawasan melekat yang dimana seluruh *supervisor* mengawasi secara langsung. Baik catatan, baik sistem, baik konfirmasi ke nasabah langsung. Jadi misalnya, yang penyaluran kredit tadi, ada kemungkinan dapat gratifikasi, kita akan me-*check* langsung ke nasabah. Kita akan melakukan konfirmasi juga ke nasabah, apakah dengan pelayanan petugas yang telah melakukan proses pencairan kredit. Nah, kemudian kita juga akan me-*check* secara sistem, seperti itu. Dan setiap 6 bulan juga atau ya, seingat saya setiap 6 bulan juga kita ada pengawasan slip untuk pegawai juga. Jadi pengawasan slip itu ketika pegawai-pegawai

melakukan pinjaman di luar nominalnya, pinjaman di luar gajinya. Itu akan menjadi *warning* bagi perusahaan. Nah, itu yang ke... itu bentuk pengawasan ya. Kemudian tadi, bagaimana mengatasi. Misalnya *pick up service* dan *delivery service*, itu kita juga ada pengawasan melekatnya. Supervisor turun tangan langsung. Nominalnya kita konfirmasi langsung juga ke nasabah pada saat penyetoran atau penarikan. Kemudian buku tabungannya juga kita cek secara langsung, dikonfirmasi oleh petugas. Jadi ketika ada kelalaian, itu seharusnya tidak bisa dilakukan oleh *personality* atau satu orang secara sistem. Nah, bagaimana kalau atasan dan anak buahnya itu melakukan... melakukan kerjasama untuk melakukan *fraud*? Makanya kita ada ketentuan *rolling session*. Jadi kita di pegawai itu ada sistem *rollingan* juga. Nah, itu berkala memang paling sering itu *teller* untuk dilakukan *rolling*. Kenapa? Karena *teller* yang langsung bersinggungan dengan nasabah. Kemudian ada juga terkait dengan proses cuti. Cuti itu kan sebenarnya kita juga bukan asal cuti. Tapi yang menggantikan itu sekaligus mengecek pekerjaan temannya. Jadi ini adalah beberapa sebagian kecil tahapan dari perusahaan untuk mengantisipasi adanya resiko-resiko potensi terjadinya *fraud* itu.

R : Baik Pak, sudah sangat jelas sekali terkait potensi sekaligus antisipasinya, Pak. Sekarang, saya akan beralih ke bagian *job desk* dari SKMR sendiri ya Pak. Nah, untuk kemarin kan untuk terkait pencegahan deteksi *fraud* itu menggunakan FDS gitu kan Pak? Ada *fraud detection system* juga. Nah, selain FDS itu kira-kira apa saja yang dilakukan untuk melaksanakan pencegahan deteksi *fraud*?

I : Oke, deteksi *fraud*, deteksi *fraud*, kalau misalnya kita bicara secara sistemnya. Itu selain FDS tentu kita ada otorisasi dan verifikasi. Jadi tidak semua pegawai itu melakukan *single authorization*. Nah, kita ada bertahap atau skala bertahap dalam melakukan otorisasi. Ketika salah satu petugas itu melakukan otorisasi tertentu, itu tidak bisa serta-merta otorisasi itu hanya di satu petugas tersebut, tapi ada tingkatannya juga, jadi ibaratnya kita ada *dual control*-nya seperti itu, atau *double check*-nya. Nah, itu yang pertama. Kemudian yang kedua sistem juga itu bisa punya *audit trail*. Jadi *audit trail* itu bagaimana sistem ini akan mengetahui siapa saja yang mengakses sistem tersebut, jam berapa bisa mengakses, dan apa yang diakses, apa yang di-*download*. Jadi semua *backend* dari sistem tersebut terbaca oleh *audit trail*. Nah, itu hal-hal yang tidak diketahui oleh petugas, karena petugas tidak punya akses tersebut. Nah, kemudian seluruh sudut ruangan kita juga dilengkapi oleh CCTV. Nah, jadi CCTV tersebut juga akan melihat bagaimana kalau misalnya ada uang fisik itu ada yang selisih khususnya di *teller*. Nah, itu juga menjadi salah satu bukti autentik untuk melihat bagaimana proses atau kejadian *event-event* tertentu yang menyebabkan adanya kekurangan, selisih, dan lain-lain itu melalui CCTV. Dan itu sangat *worth it*, sangat bermanfaat. Jadi, selain tadi *authorization*, *double check*, *dual control*, pengawasan melekat, kemudian ada proses audit, ada proses identifikasi risiko. Saya rasa cukup banyak hal-hal yang selain dengan pemanfaatan FDS.

R : Nah, tadi kan begitu banyak alat dan metodologinya ya Pak. Untuk dalam, ada nggak sih *review* dari penggunaan alat itu sendiri, kayak misalnya

kekurangannya apa di tahun ini lalu di-*upgrade* itu kira-kira berapa tahun kali sekali, Pak?

I : Kalau itu mungkin lebih ke, kalau *review* kita ada. Tapi itu sifatnya di depan ya. Jadi kita di awal kerjasama dengan pihak ketiga, tentu apa yang dikerjasamakan itu kita *review* dulu. Jadi kita *review* dulu, kita lihat perjanjian kerjasamanya secara hukum, apakah ada kekeliruan dari klausul-klausul atau mungkin ada yang berpotensi risiko dari klausul-klausul tersebut secara PKS (Perjanjian Kerja Sama). Nah, setelah kita *review*, kita cek secara data kita, apakah aman ketika diakses oleh pihak luar. Jadi biasanya kita ada NDA (*Non-Disclosure Agreement*), kemudian juga ada perjanjian kerjasamanya. Nah, itu untuk bagian depannya. Kemudian untuk belakangnya, tentu ada evaluasi. Evaluasi ini *by experience* ya. Jadi bagaimana, oh ternyata selama kita bekerja, sistem ini kurang ini, sistem itu kurang itu, masih ada celah di sini, masih ada celah di situ. Kita bahkan mungkin bukan berkala lagi mbak, kalau ada yang sudah tidak sesuai, kita akan komunikasikan ke vendor. Nah, itu langsung kita *make sure* untuk dilakukan perbaikan saat itu juga.

R : Kalau misalnya untuk penyusunan usul lagi untuk pekerjaan ataupun prosedur yang meminimalisir risiko *fraud*, apakah dari SKMR melakukan itu Pak?

I : Oh iya, tentu kita melakukan juga *review* terkait kebijakan kita juga banyak melakukan usulan. Jadi SKMR itu sebenarnya bersifat makro. Jadi kita tidak hanya menyentuh hal-hal yang kecil, tapi kita juga menjadi semacam tim analisanya untuk sebuah perusahaan. Perusahaan mau diarahkan kemana? Industrinya bergerak dimana? Jadi kalau misalnya tujuan perusahaan tidak sesuai

dengan tujuan industri, itu kita coba luruskan lagi dengan data. Oh ternyata hasil dari SKMR arah perusahaan itu terlalu beresiko. Nah, itu kita arahkan kembali, kita sarankan untuk diluruskan kembali. Dan itu kita presentasikan di direksi ya, di manajemen lah seperti itu.

R : Kalau misalnya untuk penetapan bagaimana *fraud* yang signifikan sama enggak itu kapan dan bagaimana, Pak?

I : Oke, *fraud* secara signifikan dan tidak itu kita punya komitenya. Jadi kita ada komite, di mana komite tersebut itu memang dibentuk lintas unit kerja. Jadi ada namanya kita komite anti-fraud, jadi penentuan signifikansi dan tidak signifikannya suatu kejadian *fraud*. Itu ditentukan dari hasil pembicaraan dalam komite dan tim tersebut. Tentu kita akan menimbang kerugiannya. Kita akan menimbang besarnya kasus tersebut seperti apa. Dan ya *alhamdulillah*, setau saya saat ini tidak ada yang bersignifikan.

R : Kalau untuk misalnya ada pelaporan dari indikasi *fraud* sendiri itu, apakah dari setiap pelaporan tersebut akan ditindaklanjuti atau tidak Pak?

I : Oke, jawaban singkatnya pasti ditindaklanjuti. Kita akan tindaklanjuti meskipun itu benar atau tidak. Jadi setiap pelaporan yang masih sifatnya dugaan itu pasti kita akan tindaklanjuti. Tapi kalau misalnya pada akhirnya dugaan tersebut tidak terbukti, ya *everything back to normal* gitu. Semuanya akan kita kembalikan ke normal bahwa ini tidak ada apa-apa, sesuai dengan hasil investigasi kita.

R : Berarti kalau misalnya dugaannya ternyata tidak terbukti Itu apakah tetap dibuat laporan atau tidak Pak?

I : Oke, kalau dibuat laporannya kita tetap akan membuat laporannya. Cuma sejauh mana kita akan membuktikan itu. Kadangkan kalau misalnya masih tahapan, kita kan ada tahapan-tahapannya ya. Kalau tahapannya masih di *low-middle* saya rasa sih kita masih belum membuat laporannya. Tapi kalau rasa-rasanya itu sudah menjelang benar-benar ada yang terdapat, terjadi. Meskipun ada kerugian tapi misalnya tidak menunjuk salah satu orang dan lain-lain. Nah itu kita buat laporannya.

R : Mungkin yang terakhir Pak, kalau menurut Bapak sendiri Untuk strategi anti-fraud yang diterapkan di Bank Sleman ini, apakah sudah efektif?

I : Oke, tentu kita selalu optimis bahwa kita inginnya strategi anti-fraud di Bank Sleman itu berjalan efektif terus mungkin sekarang juga bukan cuman sekedar efektif. Tapi anti-fraud juga memerlukan sebuah inovasi, sebuah sistem. Kemudian sebuah kebersamaan. Kebersamaan yang saya maksud adalah bagaimana *culture* terkait dengan anti-fraud, bukan dipahami oleh orang-orang *risk* saja, tapi oleh seluruh unit kerja, oleh seluruh pegawai bahkan oleh seluruh pekerja yang non-pegawai juga. Misalnya entah itu yang mungkin dari OB, mungkin dari satuan keamanan, dan lain-lain. Saya rasa pemahaman anti-fraud itu seluruhnya wajib dipahami oleh insan perbankan dari golongan apapun. Dan itu yang kita lakukan. Kita melakukan sosialisasi anti-fraud itu bukan cuman hanya ke bawah, bahkan sampai level tertentu, misalnya OB tadi dan lain-lain Itu juga kita sampaikan juga bahwa terkait dengan pentingnya pemahaman anti-fraud.

R : Kalau untuk di Bank Sleman sendiri berarti selama beberapa tahun terakhir apakah pernah terjadi *fraud* Pak?

I : Oke, kalau untuk beberapa tahun terakhir setahun saya, itu memang belum ada terjadi *fraud* yang secara signifikan. Dan itu memang, cuman memang kan kalau di OJK itu mau nihil itu tetap kita laporkan. Nah, jadi secara signifikan itu belum ada, *alhamdulillah*.

Appendix 8. Interview Transcript 7

Interviewee : Mr. Arif Setiawan

Interview Date : 19 February 2026

Position : Senior Internal Audit

R : Researcher

I : Interviewee/Informant

R : Apa saja potensi-potensi *fraud* yang dapat muncul dan perlu dicegah oleh penerapan Strategi Anti-Fraud di Bank Sleman Pak?

I : Potensi *fraud* yang dapat muncul meliputi *fraud* oleh pegawai atau *internal fraud*, seperti manipulasi data kredit dengan memalsukan data debitur, *mark-up* agunan, kredit fiktif, lalu penggelapan dana nasabah dengan penarikan tanpa izin, tidak menyetorkan setoran, lalu penyalahgunaan wewenang seperti meloloskan kredit bermasalah karena konflik kepentingan, pemalsuan dokumen internal dengan tanda tangan, bukti transaksi, lalu kolusi antar pegawai untuk menutupi penyimpangan. Lalu ada juga, *fraud* oleh nasabah atau *external fraud*, seperti identitas palsu saat pembukaan rekening atau pengajuan kredit, kredit macet disengaja seperti debitur tidak beritikad baik, pemalsuan dokumen pendukung kredit seperti slip gaji, laporan usaha. Ada juga *fraud* teknologi informasi atau *IT fraud*, seperti akses ilegal ke sistem perbankan, penyalahgunaan user ID dan password pegawai, manipulasi data transaksi di sistem, serangan siber seperti *phishing* dan *malware* yang merugikan bank atau nasabah. Lalu, *fraud* proses

kredit, seperti kredit fiktif atau topengan, *over-financing* seperti plafon tidak sesuai kemampuan debitur, agunan tidak sesuai nilai sebenarnya, rekayasa hasil analisis kredit yang mencakup BI Checking atau SLIK maupun *cash flow*. Ada lagi *fraud* dalam pengadaan barang dan jasa, seperti *mark-up* harga pengadaan, vendor fiktif, suap atau gratifikasi dari rekanan, pengadaan tidak sesuai spesifikasi. Lalu yang terakhir mungkin, ada *fraud* pelaporan & keuangan, seperti rekayasa laporan keuangan, menyembunyikan kredit bermasalah atau NPL, manipulasi cadangan kerugian penurunan nilai atau CKPN.

R : Apakah SKAI secara rutin menilai penerapan sistem pengendalian internal Pak?

I : Untuk SKAI tidak menangani kasus sehari-hari mbak, tetapi memastikan bahwa sistem pencegahan dan penanganan *fraud* kuat dalam unit-unit kerja.

R : Bagaimana hasil penilaian tersebut digunakan untuk memperkuat strategi anti-fraud Pak?

I : Hasil penilaian itu digunakan untuk memastikan pencegahan, deteksi, dan penanganan *fraud* berjalan efektif, sekaligus memberi *assurance* dan arah perbaikan begitu mbak.

R : Apakah masih ditemukan pengendalian yang belum efektif, Pak?

I : Untuk pengendalian masih bersifat dinamis dan terus berkembang mbak.

R : Bagaimana SKAI memastikan ketaatan unit kerja terhadap kebijakan dan prosedur Pak?

I : Untuk itu, SKAI memastikan pelaksanaan kegiatan unit kerja sesuai ketentuan internal bank, otoritas, dan perundang-undangan.

R : Apakah sering ditemukan *fraud* Pak? Lalu apakah ada kendala apa yang dihadapi dalam penegakan kepatuhan Pak?

I : Untuk pelanggaran tidak sering ditemukan mbak. Kalau untuk kendala yang dihadapi antara lain ketidakpahaman terhadap ketentuan, kurangnya ketelitian petugas, serta fungsi supervisi begitu sih mbak yang sering ditemukan.

R : Apakah *surprise audit* telah dilakukan sebagai bentuk deteksi *fraud* Pak? Lalu bagaimana efektivitasnya, dan apakah terdapat hambatan dalam pelaksanaannya Pak?

I : Oke mbak, *surprise audit* telah dilakukan sebagai bentuk deteksi *fraud* dan dinilai cukup efektif untuk jenis *fraud* yang bersifat rutin serta berbasis manipulasi proses harian. Namun, dalam pelaksanaannya terkadang terdapat hambatan berupa timing yang kurang tepat gitu mbak.

R : Bagaimana peran SKAI dalam melakukan investigasi *fraud* Pak? Lalu apakah proses pengumpulan bukti sudah berjalan optimal, dan kendala apa yang paling sering muncul dalam investigasi Pak?

I : SKAI sendiri berperan dalam menerima dan menilai indikasi *fraud*, melakukan investigasi *fraud*, menjaga independensi dan objektivitas, serta berkoordinasi dengan pihak terkait. Proses pengumpulan bukti sudah berjalan optimal. Kendala yang paling sering muncul dalam investigasi adalah tim yang kecil dan keterbatasan waktu mbak.

R : Apakah rekomendasi hasil audit ditindaklanjuti oleh unit kerja? Lalu bagaimana efektivitasnya dalam mencegah *fraud* dan hambatan apa yang menyebabkan rekomendasi sulit diterapkan Pak?

I : Rekomendasi hasil audit ditindaklanjuti oleh unit kerja dan berfungsi sebagai alat pencegahan serta *early warning* sekaligus sebagai dasar perbaikan berkelanjutan, mbak. Namun, hambatan yang dihadapi dalam penerapannya adalah kurangnya sistem monitoring tindak lanjut dari perusahaan.

R : Bagaimana SKAI menjaga kerahasiaan dokumen investigasi Pak? Apakah penyimpanan dokumentasi sudah memadai untuk *audit trail*, dan apakah terdapat kendala teknis atau administratif dalam pengelolaan dokumen Pak?

I : Untuk kerahasiaan dokumen investigasi dijaga melalui aturan yang jelas, akses terbatas, pengamanan teknis, serta integritas auditor mbak. Penyimpanan dokumentasi sudah memadai untuk *audit trail* dan tidak terdapat kendala teknis maupun administratif dalam pengelolaan dokumen.

Appendix 9. Interview Transcript 8

Interviewee : Mrs. Rizky Chitra
 Interview Date : 19 February 2026
 Position : Human Capital Staff

R : Researcher

I : Interviewee/Informant

R : Apa saja potensi-potensi *occupational fraud* yang dapat muncul dan perlu dicegah oleh penerapan Strategi Anti-Fraud di Bank Sleman Bu?

I : Potensi *occupational fraud* yang dapat muncul meliputi fraud oleh pegawai *internal fraud*, serta *fraud* teknologi informasi termasuk penyalahgunaan *user ID* dan *password* pegawai, manipulasi data transaksi di sistem, dan serangan siber seperti *phishing* dan *malware* yang merugikan bank atau nasabah. Selain itu terdapat *fraud* dalam proses kredit seperti kredit fiktif atau topengan, *over-financing* dengan plafon tidak sesuai kemampuan debitur, agunan tidak sesuai nilai sebenarnya, serta rekayasa hasil analisis kredit seperti BI Checking atau SLIK dan *cash flow*. *Fraud* dalam pengadaan barang dan jasa juga berpotensi terjadi seperti *mark-up* harga, vendor fiktif, suap atau gratifikasi dari rekanan, serta pengadaan yang tidak sesuai spesifikasi. *Fraud* pelaporan dan keuangan seperti rekayasa laporan keuangan, menyembunyikan kredit bermasalah atau NPL, serta manipulasi cadangan kerugian penurunan nilai atau CKPN juga perlu dicegah.

R : Apakah kebijakan KYE telah diterapkan sejak *proses pre-screening* dan rekrutmen bu? Lalu bagaimana pelaksanaannya dalam praktik Bu?

I : Kebijakan KYE sudah diterapkan sejak proses *pre-screening* dan rekrutmen. Dalam praktiknya dilakukan melalui pengecekan media sosial calon pegawai maupun pegawai, pengecekan SLIK calon pegawai maupun pegawai, serta adanya *coaching* antara atasan dan bawahan.

R : Kalau untuk kendala Bu, apa yang dihadapi dalam penerapan KYE sejak awal rekrutmen?

I : Untuk kendala yang dihadapi adalah tidak terbukanya calon pegawai pada saat *interview* sih mbak.

R : Bagaimana SDM mendeteksi perubahan perilaku atau kebiasaan pegawai yang mengarah pada indikasi *fraud* dan apakah mekanisme ini berjalan efektif Bu?

I : Biasanya perubahan perilaku atau kebiasaan pegawai dideteksi melalui adanya perubahan gaya hidup serta hasil laporan atau pencarian informasi dari atasan maupun *peer group*. Dan mekanisme ini dinilai efektif ya mbak.

R : Kalau untuk tantangan terbesar dalam mendeteksi indikasi *fraud* berbasis perilaku apakah ada Bu?

I : Tantangan terbesar adalah minimnya informasi yang diterima bagian SDM apabila ada indikasi *fraud* di cabang atau kantor yang berbeda, serta pegawai yang meng-*hide* atau memblokir ketika sedang berlibur atau melakukan kegiatan yang tidak seperti biasanya gitu mbak.

R : Program apa saja ya Bu yang telah dilakukan untuk meningkatkan *anti fraud awareness* dan sejauh mana program tersebut dipahami serta diikuti oleh pegawai?

I : Program yang dilakukan antara lain sosialisasi kepada seluruh karyawan, pemasangan pamflet atau *screensaver* PC terkait anti fraud di lingkungan kantor, serta penandatanganan pakta integritas, kode etik, dan deklarasi anti fraud setiap tahun. Sosialisasi diikuti dan diterapkan dengan baik, serta atasan selalu mengingatkan pada saat briefing pagi. Dan dalam pelaksanaannya sendiri sudah efektif dan tidak ada kendala mbak.

R : Bagaimana pengembangan SDM dilakukan untuk meningkatkan kewaspadaan terhadap *fraud* dan apakah pelatihan yang diberikan sudah memadai Bu?

I : Untuk pengembangan SDM dilakukan dengan rutin melakukan sosialisasi serta pelatihan terkait SAF dan pelatihan yang diberikan sudah sangat memadai mbak.

R : Kendala apa yang dihadapi dalam peningkatan kesadaran dan kehati-hatian pegawai Bu?

I : Kendala yang dihadapi adalah sistem *monitoring* dari atasan yang lemah karena terdapat beberapa manajer yang memiliki banyak anak buah sehingga *monitoring* kurang maksimal, serta kesadaran pegawai yang rendah terkait bahaya *fraud*.

Appendix 10. Interview Transcript 9

Interviewee : Mrs. Dian Chandra Dewi

Interview Date : 28 February 2026

Position : Legal Compliance, and APU PPT Staff

R : Researcher

I : Interviewee/Informant

R : Apa saja potensi-potensi *occupational fraud* yang dapat muncul dan perlu dicegah oleh penerapan Strategi *Anti-Fraud* di Bank Sleman?

I : Potensi *fraud* di bank itu biasanya mbak, meliputi korupsi, penyuapan, penerimaan tidak sah, pemerasan, penyalahgunaan aset, kecurangan laporan keuangan, penipuan, pembocoran informasi rahasia, dll.

R : Apakah kode etik dan kebijakan benturan kepentingan telah diterapkan secara menyeluruh?

I : Iya betul mbak, untuk itu sudah diterapkan secara menyeluruh.

R : Bagaimana cara memastikan seluruh pegawai mematuhi kebijakan tersebut?

I : Untuk memastikan kebijakan telah dilakukan adalah melalui sosialisasi kebijakan, menetapkan *dual control* dalam proses kerja, dan melakukan audit secara berkala pada unit kerja itu mbak.

R : Kendala apa yang dihadapi dalam penerapan budaya kerja anti fraud?

I : Untuk kendala, menurut saya setidaknya ada dua mbak. Yang pertama, pengembangan infrastruktur teknologi untuk mendukung penerapan budaya kerja anti *fraud* biasanya berbiaya mahal. Terus juga mbak, kurangnya kepercayaan karyawan terhadap manajemen dalam pelaksanaan budaya anti *fraud* juga, contohnya karyawan takut melakukan laporan *whistleblowing*, meskipun telah dilakukan sosialisasi secara rutin mengenai perlindungan bagi pelapor.

R : Apakah strategi anti *fraud* disusun dan diawasi secara menyeluruh oleh SKK?

I : Strategi anti *fraud* disusun dan diawasi oleh unit anti *fraud* mbak, sedangkan SKK bertugas memastikan strategi anti *fraud* yang disusun tidak menyimpangi ketentuan peraturan perundangan yang berlaku termasuk peraturan otoritas jasa keuangan, begitu pembagiannya.

R : Bagaimana proses penyempurnaan dan pengkinian strategi anti fraud dilakukan?

I : Untuk proses penyempurnaan dan pengkinian SAF dilakukan berdasarkan 3 hal, yaitu penyesuaian dengan peraturan perundangan dan peraturan OJK, perkembangan produk layanan bank, dan hasil evaluasi atas kasus *fraud* yang terjadi, mbak.

R : Apakah terdapat hambatan dalam menyesuaikan strategi dengan perkembangan usaha bank?

I : Hambatan dalam penyesuaian SAF dengan perkembangan usaha... ada mbak, hambatannya adalah dalam pengembangan produk diperlukan pengembangan

infrastruktur teknologi anti *fraud* contohnya FDS atau *Fraud Detection System* yang pengembangannya berbiaya mahal.

R : Bagaimana SKK memastikan bahwa strategi anti fraud dijalankan sesuai ketentuan?

I : Kalau itu dengan sosialisasi rutin kepada unit kerja melalui tatap muka maupun secara daring, dan juga memastikan tidak terdapat kasus *fraud*.

R : Apakah seluruh unit kerja sudah patuh terhadap kebijakan tersebut?

I : Bisa dikatakan begini mbak, seluruh unit kerja sudah patuh selama tidak terdapat temuan *fraud*.

R : Kendala apa yang paling sering ditemukan dalam pengawasan kepatuhan?

I : Sejauh ini, tidak ada kendala.

R : Apakah saluran komunikasi internal terkait kebijakan anti *fraud* sudah tersedia dan digunakan?

I : Sudah tersedia, seperti yang disebutkan di *interview* kemarin mbak, seperti *whistleblowing system*, portal kebijakan, dan banner atau poster *online*.

R : Bagaimana efektivitas komunikasi tersebut dalam meningkatkan pemahaman pegawai?

I : Sudah sangat efektif mbak.

R : Apakah masih ada kendala dalam penyampaian informasi anti *fraud* ke seluruh pegawai?

I : Tidak ada mbak, melalui sosialisasi dan usaha lain yang kemarin saya sebutkan sudah cukup memadai.

Appendix 11. Framework Matrix of Potential Occupational Fraud at PT BPR Bank Sleman

	RQ 1 Potential Occupational Fraud Risk	1. Asset Misappropriation	2. Corruption
Mr Arif Setiawan (9 December 2025)			
Mr Arif Setiawan (19 February 2026)		Potensi fraud yang dapat muncul meliputi fraud oleh pegawai atau internal fraud, seperti penggelapan dana nasabah dengan penarikan tanpa izin, tidak menyetorkan setoran.	penyalahgunaan wewenang seperti meloloskan kredit bermasalah karena konflik kepentingan, pemalsuan dokumen internal dengan tanda tangan, bukti transaksi, lalu kolusi antar pegawai untuk menutupi penyimpangan. manipulasi data transaksi di sistem, Ada lagi fraud dalam pengadaan barang dan jasa, seperti mark-up harga pengadaan, suap atau gratifikasi dari rekanan, pengadaan tidak sesuai spesifikasi.
Mr Dwi Handoyo Miharjo (9 December 2025)		dan ketika orang tersebut mendapatkan keuntungan secara pribadi, itu bisa kita katakan fraud. Karena kebanyakan kan, orang-orang tau fraud itu, oke saya nyuri uang, saya mengatakan itu fraud.	Tapi, fraud kan bukan cuma itu saja. Mungkin nanti mbak juga bisa mencari jawabannya, fraud itu apa saja. Tapi, misalnya kamu pembocoran rahasia, ada benturan kepentingan, itu sudah meranan ke area fraud. Jadi, itu menurut saya penting diketahui oleh seluruh unit kerja, bukan cuma unit saya sendiri.

	3. Financial Statement Fraud	4. Deception	5. Leakage of Confidential Information
Mr Arif Setiawan (9 December 2025)			
Mr Arif Setiawan (19 February 2026)	Lalu yang terakhir mungkin, ada fraud pelaporan & keuangan, seperti rekayasa laporan keuangan, menyembunyikan kredit bermasalah atau NPL, manipulasi cadangan kerugian penurunan nilai atau CKPN.	Potensi fraud yang dapat muncul meliputi fraud oleh pegawai atau internal fraud, seperti manipulasi data kredit dengan memalsukan data debitur, mark-up agunan, kredit fiktif, Lalu ada juga, kredit macet disengaja seperti debitur tidak beritikad baik, pemalsuan dokumen pendukung kredit seperti slip gaji, laporan usaha. manipulasi data transaksi di sistem, Lalu, fraud proses kredit, seperti kredit fiktif atau topengan, over-financing seperti plafon tidak sesuai kemampuan debitur, agunan tidak sesuai nilai sebenarnya, rekayasa hasil analisis kredit yang mencakup BI Checking atau SLIK maupun cash flow. Ada lagi fraud dalam pengadaan barang dan jasa, seperti mark-up harga pengadaan, vendor fiktif, suap atau gratifikasi dari rekanan, pengadaan tidak sesuai spesifikasi.	Ada juga fraud teknologi informasi atau IT fraud, seperti akses ilegal ke sistem perbankan, penyalahgunaan user ID dan password pegawai,
Mr Dwi Handoyo Miharjo (9 December 2025)		Parameternya itu misalnya seperti, oh ada transaksi ATM dilakukan secara bersamaan di selang waktu bersamaan, gitu. Jadi, itu FDS kita ngebaca itu, sistem kita ngebaca itu. Atau misalnya ada bukan nasabah tapi berhasil melakukan transaksi seperti itu. Atau ada rekening pasif tapi dapat melakukan transaksi. Jadi hal-hal yang tidak normal itu akan diketahui oleh FDS namanya, Fraud Detection System.	Jadi bukan cuma fraud terkait dengan uang, tapi fraud bagaimana pembocoran data, rahasia data, dan lain-lain. Tapi, misalnya kamu pembocoran rahasia, ada benturan kepentingan, itu sudah meranan ke area fraud. Jadi, itu menurut saya penting diketahui oleh seluruh unit kerja, bukan cuma unit saya sendiri.

	RQ 1 Potential Occupational Fraud Risk	1. Asset Misappropriation	2. Corruption
Mr Dwi Handoyo Miharjo (2 February 2026)		Yang pertama namanya kredit uang keluar Itu resikonya pasti ada salah satunya adalah fraud, dimana uang tersebut yang kita salurkan ke nasabah. Itu berpotensi dimanfaatkan oleh oknum-oknum tertentu Kemudian yang kedua juga di unit kerja lain, ada karena kita bersinggungan langsung dengan nasabah, kita punya namanya program delivery service, kemudian kita punya juga program pick up service. Dimana kalau petugas kita itu tidak memiliki integritas yang bagus, itu akan berpotensi disalahgunakan uang yang diambil atau uang yang di-pick up, uang yang di-delivery itu bisa disalahgunakan, kemudian tidak disetorkan di bank. Itu hal-hal yang sangat memungkinkan terjadi Kemudian, ya sebenarnya banyak yang di perbankan, ya itu dua contohnya. Mungkin sekaligus saya akan membahas terkait dengan antisipasinya seperti apa. Nah, jadi CCTV tersebut juga akan melihat bagaimana kalau misalnya ada uang fisik itu ada yang selisih khususnya di teller. Nah, itu juga menjadi salah satu bukti autentik untuk melihat bagaimana proses atau kejadian event-event tertentu yang menyebabkan adanya kekurangan, selisih, dan lain-lain itu melalui CCTV. Dan itu sangat worth it, sangat bermanfaat. Jadi, selain tadi authorization, double check, dual control, pengawasan melekat, kemudian ada proses audit, ada proses identifikasi risiko. Saya rasa cukup banyak hal-hal yang selain dengan pemanfaatan FDS.	Misalnya, oke karena pencairannya selesai mendapat gratifikasi, mendapat imbalan, mendapat hal-hal yang diluar ketentuan perbankan atau regulasi. Kita semua sepakat kalau gratifikasi itu juga termasuk salah satu bagian dari fraud. Jadi misalnya, yang penyaluran kredit tadi, ada kemungkinan dapat gratifikasi, kita akan me-check langsung ke nasabah. Kita akan melakukan konfirmasi juga ke nasabah, apakah dengan pelayanan petugas yang telah melakukan proses pencairan kredit. Nah, kemudian kita juga akan me-check secara sistem, seperti itu. Jadi ketika ada kelalaian, itu seharusnya tidak bisa dilakukan oleh personality atau satu orang secara sistem. Nah, bagaimana kalau atasan dan anak buahnya itu melakukan... melakukan kerjasama untuk melakukan fraud? Makanya kita ada ketentuan rolling session. Jadi kita di pegawai itu ada sistem rollingan juga. Nah, itu berkala memang paling sering itu teller untuk dilakukan rolling.

	3. Financial Statement Fraud	4. Deception	5. Leakage of Confidential Information
Mr Dwi Handoyo Miharjo (2 February 2026)			Oke, deteksi fraud, deteksi fraud, kalau misalnya kita bicara secara sistemnya. Itu selain FDS tentu kita ada otorisasi dan verifikasi. Jadi tidak semua pegawai itu melakukan single authorization. Nah, kita ada bertahap atau skala bertahap dalam melakukan otorisasi. Ketika salah satu petugas itu melakukan otorisasi tertentu, itu tidak bisa serta-merta otorisasi itu hanya di satu petugas tersebut, tapi ada tingkatannya juga, jadi ibaratnya kita ada dual control-nya seperti itu, atau double check-nya. Nah, itu yang pertama. Kemudian yang kedua sistem juga itu bisa punya audit trail. Jadi audit trail itu bagaimana sistem ini akan mengetahui siapa saja yang mengakses sistem tersebut, jam berapa bisa mengakses, dan apa yang diakses, apa yang di-download. Jadi semua backend dari sistem tersebut terbaca oleh audit trail. Nah, itu hal-hal yang tidak diketahui oleh petugas, karena petugas tidak punya akses tersebut. Nah, kemudian seluruh sudut ruangan kita juga dilengkapi oleh CCTV

	RQ 1 Potential Occupational Fraud Risk	1. Asset Misappropriation	2. Corruption
Mrs Dian Chandra Dewi (9 December 2025)		Kalau anti fraud, menurut saya yang paling rentan itu bagian yang memegang uang, kayak funding, lending, kredit, kemudian bagian teller. Bukan Cuma di Bank Sleman namun di bank lainpun juga memang di bagian itulah yang rentan terjadi fraud. Karena memang setiap hari berurusan dengan nasabah, sudah tahu karakteristik nasabah, jadi setiap hari tanggung jawabnya memang mengelola dana nasabah. Jadi yang bagian yang paling rentan itu adalah itu, dan kita tanggulangnya dengan memang kita di bagian-bagian itu kita sudah buat sistemnya. Misalkan dia mau backup dana nasabah, dia harus mencatat dulu, kemudian dia harus izin dulu ke atasannya, mau apa nasabah mana aja backup-nya, kemudian setelah selesai nanti nominalnya berapa yang dia ambil. Kemudian ketika dia akan melakukan di teller untuk transaksi, itu teller-nya juga melakukan konfirmasi, benar atau tidak, mau melakukan penarikan sebesar ini, atau benar atau tidak, buat transaksi setoran nominalnya sekian melalui akun ini. Untuk transaksi teller juga, mereka untuk transaksi nominal tertentu, mungkin kalau di kita itu sekitar 15 juta, itu harus ada approve dari atasannya, mau dia penarikan atau setoran, kemudian ada juga untuk rekeningnya, yang sudah lama tidak bertransaksi, kadang ada rekening yang memang nasabah menabung satu miliar misalnya, dan itu memang dia mau disimpan buat investasi, jadi nggak pernah ditarik atau apa, itu kan kita juga ada sistemnya langsung sebagai rekening pasif, jadi dia tidak bisa melakukan transaksi, memang nasabahnya	
Mrs Dian Chandra Dewi (28 February 2026)		penyalahgunaan aset,	Potensi fraud di bank itu biasanya mbak, meliputi korupsi, penyuapan, penerimaan tidak sah, pemerasan,

	3. Financial Statement Fraud	4. Deception	5. Leakage of Confidential Information
Mrs Dian Chandra Dewi (9 December 2025)		Nah untuk fraud sendiri kalau untuk aplikasi digital ini terkait dengan transaksi ATM dan virtual account itu kita memang ada yang namanya sistemnya Fraud Detection System, FDS ya, terus dia nempel di aplikasinya itu, disitu kita buat parameternya apa sih yang kira-kira terkait fraud itu, misal dia transaksinya di ATM yang jangkauannya jauh dari Bank Sleman, kemudian transaksinya dua kali, di ATM yang berbeda dengan jarak yang jauh, itu kan bisa menjadi parameter terjadinya fraud kayak gitu, nah itu nanti akan masuk ke FDS, jadi di FDS itu nanti otomatis akan terblokir rekeningnya, nah baru setelah itu akan dilakukan cek dari bagian fraudnya, Anti Fraud, nanti akan dicek bahwa ini transaksinya apakah memang nasabah atau bukan, kalau memang bukan nasabah, nanti akan konsultasi juga sama nasabah apakah memang ini transaksi nasabah atau bukan, kalau memang itu transaksi nasabah, maka nasabah nanti bisa kesini dan bisa melakukan penggantian ATM, soalnya mungkin ATMnya itu kalau masuk ke red flag itu ya, ini tuh apakah kalau memang nasabahnya dia nanti bisa ganti ATM atau dia bisa buka blokirnya, tapi kalau misalkan itu bukan nasabah, ya dia harus langsung ganti ATMnya, karena mungkin sudah terkena orang, ter-hack gitu ya.	itu memang kita sudah ada yang tadi ada FDS, kemudian itu juga sudah ada ketentuannya, parameternya sudah ditetapkan. Kemudian ada juga yang kita melakukan analisa transaksi tadi, yang kita menilai internetnya mencurigakan atau engga, itu di luar FDS ya. Kemudian ada juga untuk yang fraud internal, itu kita bisa melihat dari sistem itu juga, wajib terdapat audit trail. Jadi untuk semua yang masuk ke sistem, kita pasti ada user dan password, kita sudah melakukan juga untuk membuat ketentuan harus ada, untuk membalas sistem harus ada audit trail-nya, kemudian disitu harus bisa dilihat siapa yang terakhir kan mengakses, apa akses apa yang dia lakukan dan dia ubah
Mrs Dian Chandra Dewi (28 February 2026)	kecurangan laporan keuangan,	penipuan,	pembocoran informasi rahasia, dll.

	RQ 1 Potential Occupational Fraud Risk	1. Asset Misappropriation	2. Corruption
Mrs Rizky Chitra (10 December 2025)			
Mrs Rizky Chitra (22 December 2025)		Sejauh ini yang paling efektif adalah pengecekan SLIK. Karena dari SLIK dapat dilihat gaya hidup pegawai dan pinjaman yang dimiliki, seperti pinjol atau paylater yang berisiko. Rekam jejak pegawai dilakukan untuk semua calon pegawai. Apabila calon pegawai sudah pernah bekerja, maka dilakukan pengecekan ke perusahaan lama, cross check dengan bagian HRD apakah calon pegawai tersebut memiliki rekam jejak yang baik atau kurang baik di perusahaan sebelumnya. Selain itu saat ini sudah ada aplikasi SIPELAKU dari OJK sehingga bagian SDM bisa mengecek apakah calon pegawai tersebut pernah terlibat dalam tindakan fraud sebelumnya. Tujuannya untuk menghindari penerimaan pegawai yang memiliki rekam jejak yang kurang baik.	
Mrs Rizky Chitra (19 February 2026)			Fraud dalam pengadaan barang dan jasa juga berpotensi terjadi seperti mark-up harga, vendor fiktif, suap atau gratifikasi dari rekanan, serta pengadaan yang tidak sesuai spesifikasi.

	3. Financial Statement Fraud	4. Deception	5. Leakage of Confidential Information
Mrs Rizky Chitra (10 December 2025)		Terdapat punishment atau demosi, PHK bagi pegawai yang melakukan tindakan-tindakan menyimpang seperti fraud atau penipuan dan lain-lain.	
Mrs Rizky Chitra (22 December 2025)			
Mrs Rizky Chitra (19 February 2026)	Fraud pelaporan dan keuangan seperti rekayasa laporan keuangan, menyembunyikan kredit bermasalah atau NPL, serta manipulasi cadangan kerugian penurunan nilai atau CKPN juga perlu dicegah.	Selain itu terdapat fraud dalam proses kredit seperti kredit fiktif atau topengan, over-financing dengan plafon tidak sesuai kemampuan debitur, agunan tidak sesuai nilai sebenarnya, serta rekayasa hasil analisis kredit seperti BI Checking atau SLIK dan cash flow. vendor fiktif,	Potensi occupational fraud yang dapat muncul meliputi fraud oleh pegawai internal fraud, serta fraud teknologi informasi termasuk penyalahgunaan user ID dan password pegawai, manipulasi data transaksi di sistem,

	RQ 1 Potential Occupational Fraud Risk	1. Asset Misappropriation	2. Corruption
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman		Penyalahgunaan Aset a. Penyalahgunaan aset adalah perbuatan dengan maksud menguntungkan diri sendiri dan/atau orang lain secara melawan hukum dengan menyalahgunakan aset Bank dan/atau pihak lain yang dikelola dan/atau dikuasi, tanpa melalui prosedur yang berlaku di Bank dan/atau pihak lain yang menyebabkan kerugian atau potensi kerugian terhadap Bank dan/atau pihak lain. Perbuatan penyalahgunaan aset meliputi: 1) Penyalahgunaan uang tunai Contoh penyalahgunaan uang tunai antara lain namun tidak terbatas pada pencurian uang muka, pencurian uang kas, pencairan yang tidak sesuai kenyataan, penggelapan premi, penyalahgunaan klaim/dana jaminan/manfaat pensiun. 2) Penyalahgunaan persediaan Contoh penyalahgunaan persediaan antara lain namun tidak terbatas pada penyalahgunaan dan pencurian aset. 3) Penyalahgunaan aset lainnya Contoh penyalahgunaan aset lainnya antara lain namun tidak terbatas pada penggunaan pos lainnya sebagai sumber angsuran kredit dan memanfaatkan pos aset lainnya untuk pembelian kebutuhan pribadi pegawai.	Korupsi a. Korupsi adalah perbuatan dengan maksud menguntungkan suatu pihak baik secara sendiri maupun bersama dengan pihak lain, secara melawan hukum dengan menyalahgunakan pengaruhnya dalam suatu transaksi bisnis, atau penyalahgunaan posisi atau kewenangannya yang dapat menguntungkan atau merugikan nasabah, Bank dan/atau pihak lain baik secara langsung maupun tidak langsung. Perbuatan korupsi meliputi: 1) Benturan kepentingan yang merugikan Bank dan/atau nasabah Contoh benturan kepentingan yang merugikan Bank dan/atau nasabah antara lain namun tidak terbatas pada: a) Pemberian suku bunga lebih rendah kepada pemegang saham yang tidak sesuai prosedur dan ketentuan. b) Penerimaan pegawai berdasarkan hubungan kedekatan dengan pejabat Bank tanpa memperhatikan kompetensi. 2) Penyuapan Contoh penyuapan antara lain namun tidak terbatas pada pemberian suap kepada pihak ketiga untuk pengurusan perizinan 3) Penerimaan tidak sah Contoh penerimaan tidak sah antara lain namun tidak terbatas pada: a) Menerima uang, barang dan/atau manfaat dari calon debitur agar permohonan kredit/pembiayaan disetujui, b) Menerima komisi tunai maupun non tunai untuk kepentingan pribadi dari nasabah atas pencairan kredit/keringanan denda/bunga yang diterima nasabah c) Penjualan Agunan Yang Diambil Alih (AYDA) oleh pegawai Bank kepada debitur dengan harga yang tidak wajar untuk memperoleh keuntungan pribadi Pegawai, 4) Pemerasan Contoh pemerasan antara lain namun tidak terbatas pada meminta uang kepada nasabah/debitur untuk mempermudah proses kredit atau spesial rate deposito.

	3. Financial Statement Fraud	4. Deception	5. Leakage of Confidential Information
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	Kecurangan Laporan Keuangan a. Kecurangan laporan keuangan adalah kesalahan penyajian yang disengaja atau kelalaian dalam jumlah atau pengungkapan dalam laporan keuangan (termasuk off balance sheet) yang tidak sesuai dengan praktik akuntansi yang berlaku umum dan didesain untuk menguntungkan pembuat kecurangan atau merugikan konsumen, Bank dan/atau pihak lain Kecurangan laporan keuangan meliputi: 1) Melebihkan kekayaan bersih dan/atau pendapatan bersih Contoh melebihi kekayaan bersih dan/atau pendapatan bersih antara lain namun tidak terbatas pada ketidaksesuaian waktu pembukuan, pencatatan pendapatan yang tidak sesuai, tidak mengungkapkan kewajiban dan beban, ketidaksesuaian penilaian aset, dan ketidaksesuaian pengungkapan aset. 2) Mengurangi kekayaan bersih dan/atau pendapatan bersih Contoh mengurangi kekayaan bersih dan/atau pendapatan bersih antara lain namun tidak terbatas pada ketidaksesuaian waktu pembukuan, pencatatan pendapatan yang tidak sesuai, melebihi jumlah kewajiban dan beban, ketidaksesuaian penilaian aset dan ketidaksesuaian pengungkapan aset.	Penipuan adalah perbuatan oleh suatu pihak, baik secara sendiri maupun bersama pihak lain, yang bermaksud menguntungkan atau menghindari kerugian secara melawan hukum dengan memanipulasi, mengelabui, memberikan gambaran semu, menyesatkan, melakukan tipu muslihat atau kebohongan terkait produk dan/atau jasa Bank, kegiatan perdagangan atau transaksi, keadaan pasar, dan/atau harga, baik langsung maupun tidak langsung, yang merugikan atau tidak merugikan terhadap nasabah, Bank dan/atau pihak lainnya. b. Contoh penipuan antara lain namun tidak terbatas pada: 1) Menjanjikan suatu hasil tertentu yang akan diperoleh nasabah namun tidak sesuai dengan kondisi sebenarnya. 2) Debitur fiktif atau pemberian kredit kepada satu atau lebih debitur dengan menggunakan identitas palsu, atau identitas pihak lain. 3) Debitur topengan atau pemberian kredit kepada debitur menggunakan identitas asli debitur yang bersangkutan namun dana digunakan oleh pihak lain. 4) Rekayasa atau manipulasi dokumen atau informasi kredit.	Pembocoran Informasi Rahasia a. Pembocoran informasi rahasia adalah perbuatan dengan maksud menguntungkan suatu pihak, baik sendiri maupun bersama dengan pihak lain secara melawan hukum dengan menyebarkan segala informasi yang bersifat rahasia milik Bank dan/atau pihak lain kepada pihak yang tidak berkepentingan, yang dapat menguntungkan atau merugikan nasabah, Bank dan/atau pihak lain. b. Contoh pembocoran informasi rahasia antara lain namun tidak terbatas pada pemberian data pihak ketiga kepada pihak lain yang tidak memiliki kewenangan dan mengungkapkan data dan/atau informasi serta kegiatan nasabah kepada pihak tidak berwenang kecuali telah memperoleh persetujuan tertulis dari nasabah atau diwajibkan berdasarkan ketentuan peraturan perundang-undangan.

Appendix 12. Framework Matrix of Anti-Fraud Strategy Implementation at PT BPR Bank Sleman

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman			a. Kesadaran Anti Fraud (Anti Fraud Awareness) adalah upaya untuk menumbuhkan kesadaran mengenai pentingnya pencegahan Fraud bagi seluruh jajaran organisasi Bank dan berbagai pihak yang berhubungan dengan Bank. Upaya untuk menumbuhkan kesadaran Anti Fraud (Anti Fraud Awareness) dilakukan antara lain melalui:		2) Program Budaya Anti Fraud Bagi Pegawai Program budaya anti fraud bagi pegawai, melalui penyelenggaraan pelatihan yang efektif dan berkesinambungan mengenai pemahaman terkait kebijakan dan prosedur anti Fraud serta penandatanganan Pakta Integritas oleh seluruh pegawai, dengan format Pakta Integritas sesuai Lampiran 2 - Pakta Integritas. Pengkinian Pakta Integritas dilakukan secara berkala.		1) Penyusunan, Sosialisasi, dan Deklarasi Kebijakan Anti-Fraud Penyusunan dan sosialisasi deklarasi anti fraud sebagaimana diatur pada Lampiran 1 – Deklarasi Anti Fraud.

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	3) Program kepedulian dan sosialisasi kewaspadaan terhadap fraud bagi nasabah atau pihak eksternal lainnya yang disampaikan melalui antara lain namun tidak terbatas pada brosur, spanduk, poster, website dan media sosial resmi Bank Sleman.	1) Penyusunan, Sosialisasi, dan Deklarasi Kebijakan Anti-Fraud Penyusunan dan sosialisasi deklarasi anti fraud sebagaimana diatur pada Lampiran 1 – Deklarasi Anti Fraud.	2) Program Budaya Anti Fraud Bagi Pegawai Program budaya anti fraud bagi pegawai, melalui penyelenggaraan pelatihan yang efektif dan berkesinambungan mengenai pemahaman terkait kebijakan dan prosedur anti Fraud serta penandatanganan Pakta Integritas oleh seluruh pegawai, dengan format Pakta Integritas sesuai Lampiran 2 - Pakta Integritas. Pengkinian Pakta Integritas dilakukan secara berkala.	Identifikasi kerawanan 1) Identifikasi kerawanan merupakan proses manajemen risiko untuk mengidentifikasi, menganalisis, dan menilai potensi risiko terjadinya Fraud. Secara umum, identifikasi kerawanan ditujukan untuk mengidentifikasi risiko terjadinya Fraud yang melekat pada setiap aktivitas yang berpotensi merugikan Bank. 2) Hasil identifikasi didokumentasikan dan diinformasikan kepada pihak yang berkepentingan dan selalu dikinikan terutama terhadap aktivitas yang dinilai berisiko tinggi untuk terjadinya Fraud.				Kebijakan mengenal Pegawai/Know Your Employee (KYE) Sebagai upaya pencegahan terjadinya Fraud, kebijakan Know Your Employee merupakan upaya pengendalian dari aspek SDM. Kebijakan Know Your Employee yang dimiliki Bank paling kurang mencakup:

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	1) Sistem dan prosedur penerimaan atau rekrutmen yang efektif, yang dapat memberikan gambaran mengenai rekam jejak calon pegawai secara lengkap dan akurat; 2) Sistem seleksi yang dilengkapi kualifikasi yang tepat dengan mempertimbangkan risiko, serta ditetapkan secara obyektif dan transparan. Sistem tersebut harus menjangkau pelaksanaan promosi maupun mutasi, termasuk penempatan pada posisi yang memiliki risiko tinggi terhadap Fraud.	3) Kebijakan “mengenal pegawai” (Know Your Employee) antara lain mencakup pengenalan dan pemantauan karakter, perilaku, dan gaya hidup pegawai. 4) Kebijakan KYE tertuang pada Pedoman Pelaksanaan Tugas Bagian SDM.	2) Sistem seleksi yang dilengkapi kualifikasi yang tepat dengan mempertimbangkan risiko, serta ditetapkan secara obyektif dan transparan. Sistem tersebut harus menjangkau pelaksanaan promosi maupun mutasi, termasuk penempatan pada posisi yang memiliki risiko tinggi terhadap Fraud.	Kebijakan dan mekanisme penanganan pengaduan (whistleblowing) 1) Perlindungan pelapor fraud dengan menjamin kerahasiaan identitas pelapor fraud serta pelaksanaan pemeriksaan dan pengungkapan atas laporan yang disampaikan. Bank memberikan penghargaan kepada pelapor fraud yang laporannya terbukti benar dan didukung bukti yang memadai. 2) Regulasi terkait pengaduan fraud, mengacu pada ketentuan dan peraturan perundang-undangan yang berlaku. 3) Sistem pelaporan fraud serta mekanisme tindak lanjutnya diatur dalam pedoman whistleblowing yang terpisah dari ketentuan ini.	Pemeriksaan mendadak (surprise audit) Surprise audit merupakan audit yang dilakukan secara tiba-tiba dan tanpa pemberitahuan sebelumnya, dapat dilakukan oleh auditor eksternal atau audit internal. Adanya surprise audit mendorong seluruh pihak Bank bersikap waspada dan melaksanakan tugas sesuai prosedur. Surprise audit dapat dilaksanakan oleh audit internal atau pihak ketiga dengan mempertimbangkan kompetensi dan independensi.	Mekanisme surprise audit yang dilakukan oleh audit internal, sbb: 1) Perencanaan, 2) Pelaksanaan pemeriksaan, 3) Pelaporan hasil pemeriksaan, 4) Tindak Lanjut hasil pemeriksaan.

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	Mekanisme surprise audit yang dilakukan oleh audit internal, sbb: 1) Perencanaan, 2) Pelaksanaan pemeriksaan, 3) Pelaporan hasil pemeriksaan, 4) Tindak Lanjut hasil pemeriksaan.		Surprise audit merupakan audit yang dilakukan secara tiba-tiba dan tanpa pemberitahuan sebelumnya, dapat dilakukan oleh auditor eksternal atau audit internal.	Sistem Pengawasan (surveillance system) Sistem pengawasan (surveillance system) merupakan suatu tindakan pengujian atau pemeriksaan yang dilakukan secara rahasia tanpa diketahui atau disadari oleh pihak yang diuji atau diperiksa dalam rangka memantau dan menguji efektifitas kebijakan anti Fraud. Sistem pengawasan dapat dilakukan oleh auditor eksternal atau audit internal secara berkala atau sewaktu-waktu apabila diperlukan.		

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman					Investigasi Investigasi dilakukan untuk mengumpulkan bukti yang terkait dengan kejadian yang patut diduga merupakan tindakan fraud. Investigasi merupakan bagian penting dalam sistem pengendalian fraud yang memberikan pesan kepada setiap pihak terkait bahwa setiap indikasi tindakan fraud yang terdeteksi selalu diproses sesuai standar investigasi dan pelaku diproses sesuai ketentuan. Standar investigasi yang dimiliki Bank paling sedikit mencakup: 2) Mekanisme pelaksanaan investigasi untuk menindaklanjuti hasil deteksi dengan tetap menjaga kerahasiaan informasi yang diperoleh.

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	1) Penentuan pihak yang berwenang melaksanakan investigasi dengan memperhatikan independensi dan kompetensi yang dibutuhkan. Kompetensi atau keahlian yang dibutuhkan antara lain: a) Analisis dan investigasi b) Akuntansi forensik Akuntansi forensik merupakan teknik dalam melakukan evaluasi dan investigasi secara rinci dan menyeluruh terhadap permasalahan keuangan yang diinvestigasi dengan menggunakan standar dan aturan. c) Komputer forensik Komputer forensik merupakan teknik untuk melakukan investigasi dan analisis melalui pengumpulan dan penyajian bukti data yang ada dalam komputer. d) Pekerjaan lapangan dan wawancara Pekerjaan lapangan merupakan proses investigasi untuk mendapatkan keyakinan secara sistematis melalui pengumpulan bukti secara objektif.		Mekanisme pelaporan dalam pelaksanaan strategi anti fraud adalah sebagai berikut:		a) Penyampaian pedoman penerapan strategi anti fraud kepada Otoritas Jasa Keuangan. b) Penyampaian perubahan pedoman penerapan strategi anti fraud (apabila ada) kepada Otoritas Jasa Keuangan dalam jangka waktu paling lama 7 (tujuh) hari kerja terhitung sejak perubahan dilakukan. c) Laporan penerapan Strategi Anti Fraud dengan periode semesteran setiap tahun serta laporan koreksi penerapan Strategi Anti Fraud (apabila ada) kepada Otoritas Jasa Keuangan. Pedoman penyampaian dan koreksi laporan penerapan strategi anti fraud mengacu pada Peraturan Otoritas Jasa Keuangan yang berlaku. d) Laporan kejadian fraud berdampak signifikan dalam jangka waktu paling lama 3 (tiga) hari kerja setelah diketahui terjadinya Fraud yang berdampak signifikan. Pelaporan kejadian fraud berdampak signifikan kepada Otoritas Jasa Keuangan dengan mengacu pada Pedoman Pengisian Laporan Fraud Berdampak Signifikan. Laporan Fraud berdampak signifikan memuat kejadian Fraud yang diperkirakan berdampak negatif secara signifikan terhadap bank dan/atau nasabah, antara lain: (1) pelanggaran signifikan terhadap ketentuan peraturan perundang-undangan yang dilakukan oleh pelaku Fraud, (2) kejadian Fraud yang dapat membahayakan kelangsungan usaha Bank, dan/atau (3) kejadian Fraud yang berpotensi menjadi perhatian publik atau menurunkan reputasi bank. 2) Penanggung jawab pelaporan dalam pelaksanaan strategi anti fraud termasuk penetapan fraud berdampak signifikan/tidak signifikan adalah Tim Penerapan Strategi Anti Fraud.

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	Pengenaan Sanksi Bank menerapkan mekanisme pengenaan sanksi yang efektif, adil, transparan dan konsisten serta menimbulkan efek jera bagi pelaku fraud dengan memperhatikan Peraturan Perusahaan dan peraturan perundang-undangan yang berlaku.	Pemantauan Pemantauan tindak lanjut atas laporan fraud sesuai dengan ketentuan internal Bank dan perundang-undangan		Evaluasi Memelihara data kejadian fraud yang bermanfaat untuk identifikasi dan evaluasi kelemahan dan penyebab terjadinya fraud serta perbaikan yang diperlukan atas manajemen risiko fraud dan pengendalian internal. Data kejadian tersebut dapat digunakan sebagai alat bantu evaluasi. Data kejadian fraud mencakup data dan informasi sebagai berikut: 1) pelaku Fraud; 2) jabatan pelaku Fraud pada saat melakukan Fraud; 3) status tindak lanjut penanganan Fraud; 4) jenis Fraud; 5) aktivitas terkait Fraud; 6) deskripsi Fraud atau modus operandi; 7) lokasi kejadian Fraud; 8) divisi/bagian terjadinya Fraud; 9) pihak yang dirugikan; 10) waktu kejadian Fraud; 11) jumlah kerugian; 12) penyebab Fraud; 13) tindakan untuk penanganan Fraud; dan 14) tindakan perbaikan untuk pencegahan Fraud. Berdasarkan data kejadian fraud dan hasil evaluasi dapat diidentifikasi kelemahan dan penyebab terjadinya fraud serta ditentukan langkah-langkah perbaikan yang diperlukan, termasuk memperkuat sistem pengendalian intern. Evaluasi menyeluruh terhadap sistem pengendalian Fraud dilakukan secara berkala.		

	1. Follow-Up Actions	i. Provisions Update	ii. Refreshment
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman	Tindak lanjut Menyusun tindak lanjut berdasarkan hasil evaluasi atas kejadian Fraud untuk memperbaiki kelemahan dan memperkuat sistem pengendalian internal agar dapat mencegah terulangnya kembali Fraud karena kelemahan yang serupa.		

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Mr Arif Setiawan (9 December 2025)				Jadi kalau dari Internal Audit kita kan juga masuk di tim SAF (Tim Strategi Anti Fraud) ya. Jadi kita bareng misalnya dari unit-unit kerja itu kan juga sudah menjalankan, kemudian dari Satuan Kepatuhan, Manajemen Risiko, juga kita dari Internal Audit itu kan kita lebih ke istilahnya setelah misalnya ada kejadian, biasanya seperti itu. Jadi kalau misalnya ada indikasi fraud ini kita biasanya nunggu tugas dari dirut, kalau misalnya ada penugasan baru kita terima seperti itu. Untuk mekanisme sekarang, kemudian juga untuk fraud, kemudian kita sudah membentuk tim, kita juga berusaha untuk melengkapi instrumen yang diperlukan, seperti ada SOP dengan pelaksanaan di unit-unit kerja. Kemudian ada ketentuan-ketentuan mungkin dari Satuan Kerja Kepatuhan (SKK) yang harus dipatuhi, pun dari tim Manajemen Risiko juga sudah rutin untuk memitigasi keadaan risiko-risiko, atau peluang-peluang yang bisa membuka celah ke depannya fraud. Itu insya Allah untuk Bank Sleman sudah cukup bagus menurut saya.	Untuk seluruh pegawai kita sudah ada ketentuannya, jadi minimal satu kali untuk seluruh pegawai itu ada pelatihan tentang SAF, sekarang wajib itu SAF, selain ada APU-PPT dan sekarang ada yang konsumen, perlindungan konsumen itu juga sama. Jadi itu sudah ada ketentuan kalau satu kali harus wajib seperti perlindungan konsumen. Dan kalau untuk Internal Audit sendiri, kita setiap ada hal-hal baru, kaitannya dengan audit, kita dapat ketentuan baru, biasanya kita juga nanti kita mengikuti untuk pelatihannya, yaitu nanti yang diadakan dari kantor sendiri, atau mungkin dari luar kita ngirim peserta ke sana. Dua-duanya, tapi biasanya lebih banyak langsung studi kasus ya, kayak aku dulu belajar juga kan, kita bisa lebih paham kalau ada langsung contoh implementasinya, jadi ya sudah tahu kok, bedanya seperti ini, teori seperti ini, jadi bisa lebih memahami.	Sejauh ini sangat membantu, jadi kita pun alhamdulillah untuk tim SKAI Bank Sleman, itu kita tiga orang, jadi ada kepala SKAI, kemudian staff-nya dua. Itu kebanyakan sudah kita ikutkan untuk sertifikasi juga, sertifikasi khusus untuk PE, jadi Pejabat Eksekutif Audit Internal. Istilahnya kita sudah ada kompetensi juga. Untuk Internal Audit, yang saya ikuti itu banyak ada audit investigatif, kemudian, misalnya kaitannya dengan audit IT, biasanya lebih ke ini sih, apa ya, yang isu-isu baru juga sih ketentuan-ketentuan baru, seperti itu, saya baru setahun juga. Kemarin ikutnya juga investigatif, kemudian juga, istilahnya itu tadi sertif, sertif kan lebih umum ya, ada perundang-undangan, kemudian juga tata kelola dan audit internalnya sendiri.	Untuk mekanisme sekarang, kemudian juga untuk fraud, kemudian kita sudah membentuk tim, kita juga berusaha untuk melengkapi instrumen yang diperlukan, seperti ada SOP dengan pelaksanaan di unit-unit kerja. Kemudian ada ketentuan-ketentuan mungkin dari Satuan Kerja Kepatuhan (SKK) yang harus dipatuhi, pun dari tim Manajemen Risiko juga sudah rutin untuk memitigasi keadaan risiko-risiko, atau peluang-peluang yang bisa membuka celah ke depannya fraud. Itu insya Allah untuk Bank Sleman sudah cukup bagus menurut saya.
Mr Arif Setiawan (19 February 2026)							
Mrs Rizky Chitra (10 December 2025)					Untuk saat ini belum ada, yang diwajibkan saat ini adalah pelatihan strategi anti fraud bagi seluruh pegawai. Tim Anti Fraud secara berkala melakukan sosialisasi terkait SAF. Apakah pelatihan diadakan dengan bekerja sama dengan pihak pemerintahan atau swasta? Dan seberapa rutin pelatihan dilakukan? I : Pelatihan SAF dilakukan sekali setiap tahun oleh narasumber, baik perorangan atau instansi swasta. Sosialisasi SAF dilakukan secara berkala oleh tim SAF. R : Bagaimana mekanisme evaluasinya? I : Mekanisme evaluasi berupa kuis setelah dilakukan sosialisasi oleh tim SAF tadi.		

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Mr Arif Setiawan (9 December 2025)	Kita harus senantiasa mendorong semua karyawan ya, misalnya semua yang ada di sini untuk budaya anti fraud. Paling nggak ada berapa TV, itu kan setiap hari menampilkan zero fraud. Kemudian juga dari masing-masing unit kerja, juga ada sosialisasi. Kemudian dari Tim Anti Fraud sendiri itu ada rutin, jadi kita sosialisasi, share refreshment, kaitannya dengan anti fraud.	Kita harus senantiasa mendorong semua karyawan ya, misalnya semua yang ada di sini untuk budaya anti fraud. Paling nggak ada berapa TV, itu kan setiap hari menampilkan zero fraud. Kemudian juga dari masing-masing unit kerja, juga ada sosialisasi. Kemudian dari Tim Anti Fraud sendiri itu ada rutin, jadi kita sosialisasi, share refreshment, kaitannya dengan anti fraud.						
Mr Arif Setiawan (19 February 2026)								
Mrs Rizky Chitra (10 December 2025)								

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Mr Arif Setiawan (9 December 2025)			Agak lama sih, sesuai kebutuhan sih, jadi kalau memang ada rotasi atau apa, ya kemungkinan, tapi kalau yang kemarin, ya itu agak lumayan lama.	Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa.		Kalau yang biasanya kita lakukan sebenarnya kan untuk audit kan memang tujuannya juga sebagian besar untuk deteksi fraud ya, jadi kalau kita memang awal kan kita harus merencanakan. Jadi untuk membuat perencanaan itu, kita kalau sekarang itu biasanya untuk memeriksa itu berdasar dari tingkat risiko, sebenarnya tingkat risiko fraud atau yang kemungkinan hal-hal yang rentan terjadi penyalahgunaan atau penyelewengan itu kita buat untuk ininya, untuk perencanaannya. Nanti setelah perencanaan kita juga harus tahu ruang lingkupnya, nanti objeknya atau fokusnya yang harus kita periksa itu apa saja, seperti itu. Lalu nanti untuk pelaksanaannya setelah nanti kita pelaksanaan untuk pemeriksaan, yang kita tahu ya mungkin nanti kita ada evaluasi juga, mungkin ada penyimpangan atau tidak kesesuaian, kita biasanya memberikan rekomendasi atau tindak lanjut. Nanti setelah dari unit itu melakukan tindak lanjutnya ya kita juga cek lagi, sampai sejauh mana dilaksanakan dari tindak lanjut dari rekomendasi dari audit. Jadi kalau yang terjadi di Bank Sleman, kita kan sudah membuat rencana untuk satu tahun ya, itu kan sudah untuk pemeriksaan khusus unit-unit kerja. Tapi kalau untuk yang kas opname, itu sudah rutin, jadi selain kita yang audit tentang kerja dengan unit-unit kerja itu, tetap yang kas opname kita jalankan setiap bulan, jadi bareng istilahnya itu.
Mr Arif Setiawan (19 February 2026)						
Mrs Rizky Chitra (10 December 2025)	Kompetensi kemampuan analytic thinking, kemampuan komunikasi yang baik, dan juga pendalaman pemahaman terkait hukum. Pada saat proses seleksi, tim SDM melakukan screening melalui media sosial dan SLIK BI, selain itu tim SDM melakukan verifikasi dengan perusahaan sebelumnya, apabila pernah bekerja sebelumnya, atau verifikasi dengan pihak yang mereferensikan.	Untuk pegawai yang sudah masuk, tim SDM melakukan pemeriksaan SLIK BI secara berkala dan pemantauan media sosial maupun gaya hidup selama di kantor.	Rotasi dilakukan 3 sampai 5 tahun sekali. Turnover cukup rendah ya, rata-rata 1 sampai 2 pegawai per tahun, dengan jumlah pegawai 170 orang.			

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Mr Arif Setiawan (9 December 2025)	Kalau fraud kita biasanya kalau dari audit itu lebih ke ini ya, kita kan biasanya ada pengawasan, jadi ada pengawasan itu istilahnya kita mengadakan pemeriksaan, jadi sampai bagaimana SOP-nya dijalankan. Kemudian ada misalnya deteksi, misalnya kita melakukan investigasi juga, misalnya dari proses ada pola-pola yang tidak sesuai seperti itu. Kita juga konsultatif, jadi misalnya dari pelaksanaan dari masing-masing unit kerja itu ada hal-hal yang rentan atau apa, biasanya kita memberikan rekomendasi seperti itu, biar lebih bagus atau lebih kuat, fraud awareness-nya. Kalau yang biasanya kita lakukan sebenarnya kan untuk audit kan memang tujuannya juga sebagian besar untuk deteksi fraud ya, jadi kalau kita memang awal kan kita harus merencanakan. Jadi untuk membuat perencanaan itu, kita kalau sekarang itu biasanya untuk memeriksa itu berdasar dari tingkat risiko, sebenarnya tingkat risiko fraud atau yang kemungkinan hal-hal yang rentan terjadi penyalahgunaan atau penyelewengan itu kita buat untuk ininya, untuk perencanaannya. Nanti setelah perencanaan kita juga harus tahu ruang lingkupnya, nanti objeknya atau fokusnya yang harus kita periksa itu apa saja, seperti itu. Lalu nanti untuk pelaksanaannya setelah nanti kita pelaksanaan untuk pemeriksaan, yang kita tahu ya mungkin nanti kita ada evaluasi juga, mungkin ada penyimpangan atau tidak kesesuaian, kita biasanya memberikan rekomendasi atau tindak lanjut. Nanti setelah dari unit itu melakukan tindak lanjutnya ya kita juga cek lagi, sampai sejauh mana dilaksanakan dari tindak lanjut dari rekomendasi dari audit.	Kalau yang penting kita setiap bulan pasti minimal ada satu kali kas opname ya, jadi terutama untuk kas besar, di brankas itu ya kita berusaha untuk itu, surprise audit kita cek, kemudian juga kaitannya inventaris seperti tabungan, materai, dan lain-lain itu juga kita cek, minimal itu sih. R : Berarti rutin sebulan sekali ya, Pak? I : Iya, cuman ya memang kita berusaha untuk kapan atau waktunya itu ya acak lah, soalnya kan ya kaitannya kan memang kas, nominal. R : Apakah hanya dilakukan di kantor pusat atau ada kemungkinan di kantor cabang juga, Pak? I : Di semua, di semua kantor cabang juga kita periksa, misalkan kebetulan kalau pas jadwalnya untuk kerja misalnya kita periksa cabang, itu ya di kantor kas juga kita ajak, jadi kita on the spot ke sana. R : Apakah ada indikator untuk melakukan surprise audit, untuk menentukan kantor mana yang diperiksa? I : Setiap bulan kita periksa semuanya. R : Berarti tidak ada indikator tertentu ya, Pak? I : Ya, istilahnya untuk penjagaan awalan juga kita setiap bulan, soalnya kan ya apa ya, itu tadi untuk kita perbankan kan, ini ya utama kan kas ya, jadi istilahnya itu untuk pemeriksaannya lebih. Jadi kalau yang terjadi di Bank Sleman, kita kan sudah membuat rencana untuk satu tahun ya, itu kan sudah untuk pemeriksaan khusus unit-unit kerja. Tapi kalau untuk yang kas opname, itu sudah rutin, jadi selain kita yang audit tentang kerja dengan unit-unit kerja itu, tetap yang kas opname kita jalankan setiap bulan, jadi bareng istilahnya itu.	Memang kan kita tetap harus menyesuaikan, itu pun juga selain kita dari internal untuk pemeriksaan misalnya IT, kita pun juga ada pemeriksaan dari eksternal, yaitu biasanya 3 tahun sekali apa ya, jadi kita juga ada, kita tetap diaudit juga dari eksternal, kaitannya dengan IT. Dan untuk auditnya sendiri, bagian Audit Internal kita, itu juga nanti juga ada dari eksternal, sampai sejauh mana kita pelaksanaannya.			Kalau fraud kita biasanya kalau dari audit itu lebih ke ini ya, kita kan biasanya ada pengawasan, jadi ada pengawasan itu istilahnya kita mengadakan pemeriksaan, jadi sampai bagaimana SOP-nya dijalankan. Kemudian ada misalnya deteksi, misalnya kita melakukan investigasi juga, misalnya dari proses ada pola-pola yang tidak sesuai seperti itu. Kita juga konsultatif, jadi misalnya dari pelaksanaan dari masing-masing unit kerja itu ada hal-hal yang rentan atau apa, biasanya kita memberikan rekomendasi seperti itu, biar lebih bagus atau lebih kuat, fraud awareness-nya.
Mr Arif Setiawan (19 February 2026)						
Mrs Rizky Chitra (10 December 2025)						

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Mr Arif Setiawan (9 December 2025)	Lebih ke IT ya, istilahnya kan kalau untuk transaksi memang kita pasti juga ngecek, untuk di SKAI itu ada yang basic-nya IT juga, jadi untuk transaksi-transaksi kita ada log user dan sebagainya itu tetap kita cek juga. Tapi misalnya ada pola-pola yang istilahnya, ya tidak normal lah istilahnya dan kita sudah dicek di sistem juga.	Ya, kita pakai ini, sesuai SOP dan job desc, kita sesuaikan. Jadi khusus unit kerja kan pasti ada, setiap bagian ada job desc. Kemudian untuk melaksanakan sesuatu itu ada SOP, ini kita sesuaikan, apakah sudah sesuai dengan ketentuan, kepatuhan tersebut. Biasanya kalau tidak sesuai, ini kan ada peluang, ada peluang yang kemungkinan nanti bisa menimbulkan fraud.			
Mr Arif Setiawan (19 February 2026)					
Mrs Rizky Chitra (10 December 2025)			Untuk pegawai yang sudah masuk, tim SDM melakukan pemeriksaan SLIK BI secara berkala dan pemantauan media sosial maupun gaya hidup selama di kantor.		

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Mr Arif Setiawan (9 December 2025)	Jadi kalau dari Internal Audit kita kan juga masuk di tim SAF (Tim Strategi Anti Fraud) ya. Jadi kita bareng misalnya dari unit-unit kerja itu kan juga sudah menjalankan, kemudian dari Satuan Kepatuhan, Manajemen Risiko, juga kita dari Internal Audit itu kan kita lebih ke istilahnya setelah misalnya ada kejadian, biasanya seperti itu. Jadi kalau misalnya ada indikasi fraud ini kita biasanya nunggu tugas dari dirut, kalau misalnya ada penugasan baru kita terima seperti itu. Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa. Untuk menjaga independensi kan kita tidak boleh terlibat di operasional langsung, jadi kebetulan kalau di bagian lain, dulu saya masih di analis itu bisa jadi tim pengadaan dan sebagainya, tapi kalau kita sudah di Audit Internal, kita tidak bisa terlibat untuk menjaga independensi. Kalaupun mau memeriksa pun, misalnya saya dari bagian analis, saya mau memeriksa bagian yang saya sebelumnya, kita juga sesuai ketentuannya, di OJK pun harus ada minimanya beberapa bulan baru bisa masuk periksa. Kalau untuk kriterianya, yang pertama integritas dan independensi, kemudian kita punya kemampuan analisa seperti itu, yang kaitannya dengan audit.	Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa. Tadi kalau untuk pengumpulan bukti kan kita bisa dari dokumen, kemudian dari on the spot, kemudian wawancara langsung bisa, kemudian dari transaksi, misalnya dari vouching seperti itu.		Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa.	Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa.
Mr Arif Setiawan (19 February 2026)					
Mrs Rizky Chitra (10 December 2025)					

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Mr Arif Setiawan (9 December 2025)	Kalau dari Internal Audit kita cuma merekomendasikan, jadi untuk sanksi, kita ya sesuai, kita rekomendasikan sesuai dengan peraturan perusahaan. Kalau untuk keputusan, kita sudah ada, yang terkait dengan SDM, sudah urusan SDM sendiri, jadi yang kita serahkan dulu dengan komisaris.	Kalau yang biasanya kita lakukan sebenarnya kan untuk audit kan memang tujuannya juga sebagian besar untuk deteksi fraud ya, jadi kalau kita memang awal kan kita harus merencanakan. Jadi untuk membuat perencanaan itu, kita kalau sekarang itu biasanya untuk memeriksa itu berdasar dari tingkat risiko, sebenarnya tingkat risiko fraud atau yang kemungkinan hal-hal yang rentan terjadi penyalahgunaan atau penyelewengan itu kita buat untuk ininya, untuk perencanaannya. Nanti setelah perencanaan kita juga harus tahu ruang lingkupnya, nanti objeknya atau fokusnya yang harus kita periksa itu apa saja, seperti itu. Lalu nanti untuk pelaksanaannya setelah nanti kita pelaksanaan untuk pemeriksaan, yang kita tahu ya mungkin nanti kita ada evaluasi juga, mungkin ada penyimpangan atau tidak kesesuaian, kita biasanya memberikan rekomendasi atau tindak lanjut. Nanti setelah dari unit itu melakukan tindak lanjutnya ya kita juga cek lagi, sampai sejauh mana dilaksanakan dari tindak lanjut dari rekomendasi dari audit.				
Mr Arif Setiawan (19 February 2026)						
Mrs Rizky Chitra (10 December 2025)	Terdapat punishment atau demosi, PHK bagi pegawai yang melakukan tindakan-tindakan menyimpang seperti fraud atau penipuan dan lain-lain.				Evaluasi kinerja dilakukan setiap semester melalui sistem KPI.	

	1. Follow-Up Actions	i. Provisions Update	ii. Refreshment
Mr Arif Setiawan (9 December 2025)	Kalau yang biasanya kita lakukan sebenarnya kan untuk audit kan memang tujuannya juga sebagian besar untuk deteksi fraud ya, jadi kalau kita memang awal kan kita harus merencanakan. Jadi untuk membuat perencanaan itu, kita kalau sekarang itu biasanya untuk memeriksa itu berdasar dari tingkat risiko, sebenarnya tingkat risiko fraud atau yang kemungkinan hal-hal yang rentan terjadi penyalahgunaan atau penyelewengan itu kita buat untuk ininya, untuk perencanaannya. Nanti setelah perencanaan kita juga harus tahu ruang lingkupnya, nanti objeknya atau fokusnya yang harus kita periksa itu apa saja, seperti itu. Lalu nanti untuk pelaksanaannya setelah nanti kita pelaksanaan untuk pemeriksaan, yang kita tahu ya mungkin nanti kita ada evaluasi juga, mungkin ada penyimpangan atau tidak kesesuaian, kita biasanya memberikan rekomendasi atau tindak lanjut. Nanti setelah dari unit itu melakukan tindak lanjutnya ya kita juga cek lagi, sampai sejauh mana dilaksanakan dari tindak lanjut dari rekomendasi dari audit. Kalau kita kan di awalkan, kalau ada indikasi kan dari whistleblower, kalau nggak, ada pelaporan, itu misalnya kita apa ya, untuk awal kita menunggu perintah dari dirut. Jadi kalau ada dari dirut nanti sudah turun penugasan, timnya siapa aja, kita nanti dari, misalkan audit ya, kita laksanakan. Nanti itu baru kita merencanakan investigasinya seperti apa, role input-nya, kemudian timeline-nya seperti apa. Kemudian kita selanjutnya kita istilahnya mengumpulkan buktinya, mau operasi ke lapangan, kita data analisis dan sebagainya, kemudian nanti kita analisa dari bukti-bukti itu, kita simpulkan fakta ringkasnya seperti apa. Kemudian kronologinya dan mungkin ada potensi kerugian atau lain-lain, baru kita laporkan ke dirut, dan nanti untuk laporannya kan, ada apa ya, tetap ada kita laksanakan ke dirut, kita laporkan ke Dewan Komisaris melalui Komite Audit, dan kemudian nanti juga tembusan ke Dirkep, Kepatuhan, dan nanti lapor ke OJK. Cuma nanti ya jika kita disitu juga ada rekomendasi, rekomendasi jadi hasilnya seperti apa.		
Mr Arif Setiawan (19 February 2026)			
Mrs Rizky Chitra (10 December 2025)			

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Mrs Rizky Chitra (22 December 2025)					R : Bagaimana perencanaan pelatihan tahunan disusun? I : Berdasarkan risiko lalu evaluasi kinerja serta usulan dari setiap unit kerja. Sejauh ini untuk pelatihan masih bersifat teoritis. Karena tim anti fraud masih cukup baru maka saat ini masih berfokus pada teori agar pegawai lebih memahami teorinya terlebih dahulu. R : Apa kelebihan dan kekurangannya? I : Kelebihannya pegawai paham mengenai teori dan regulasi. Kekurangannya pegawai belum dapat terjun praktik apabila terjadi fraud. R : Dalam satu tahun terakhir, berapa kali pelatihan tersebut dilakukan untuk masing-masing jenis dan materi yang termasuk ke dalam pelatihan pencegahan dan pendeteksian fraud? I : Untuk tahun 2025 sudah dilakukan satu kali pelatihan untuk seluruh unit kerja dan satu kali sosialisasi internal untuk seluruh pegawai. Namun ada beberapa pegawai yang mengikuti online training. R : Pihak mana yang ditunjuk oleh Bank Sleman sebagai narasumber dalam pelatihan yang tersebut? I : Bank Sleman bekerjasama dengan lembaga swasta ataupun perorangan sebagai narasumber dalam pelatihan SAF. Apabila tidak ada perubahan atau tidak diterapkan di unit terkait. Di Bank Sleman untuk setiap pelatihan wajib dilakukan pre-test dan post-test untuk mengukur keseriusan peserta pada saat mengikuti pelatihan.		Terdapat SOP terkait penerapan dan kekurangan mungkin bisa ditanyakan ke bagian kepatuhan selaku pembuat kebijakan atau review kebijakan.
Mrs Rizky Chitra (19 February 2026)							

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Mrs Rizky Chitra (22 December 2025)	Saat ini untuk membangun budaya anti fraud, tim SAF sudah melakukan antara lain, sosialisasi di setiap bagian, penggantian wallpaper setiap desktop terkait bahaya fraud, pembacaan kode etik bankir pada saat morning briefing, pemasangan poster-poster yang berisikan reminder akan bahaya fraud, dan lain-lain.	Saat ini untuk membangun budaya anti fraud, tim SAF sudah melakukan antara lain, sosialisasi di setiap bagian, penggantian wallpaper setiap desktop terkait bahaya fraud, pembacaan kode etik bankir pada saat morning briefing, pemasangan poster-poster yang berisikan reminder akan bahaya fraud, dan lain-lain.	lalu ada penandatanganan pakta integritas juga setiap tahun.					Sejauh ini yang paling efektif adalah pengecekan SLIK. Karena dari SLIK dapat dilihat gaya hidup pegawai dan pinjaman yang dimiliki, seperti pinjol atau paylater yang berisiko.
Mrs Rizky Chitra (19 February 2026)								

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Mrs Rizky Chitra (22 December 2025)	Prosedur rekrutmen sama seperti rekrutmen bagian lain. Diawali dengan seleksi dokumen lalu interview user lalu psikotes atau tes kemampuan dasar, medical check up, dan interview direksi. Terdapat SOP tertulis terkait hal tersebut. Rekam jejak pegawai dilakukan untuk semua calon pegawai. Apabila calon pegawai sudah pernah bekerja, maka dilakukan pengecekan ke perusahaan lama, cross check dengan bagian HRD apakah calon pegawai tersebut memiliki rekam jejak yang baik atau kurang baik di perusahaan sebelumnya. Selain itu saat ini sudah ada aplikasi SIPELAKU dari OJK sehingga bagian SDM bisa mengecek apakah calon pegawai tersebut pernah terlibat dalam tindakan fraud sebelumnya. Tujuannya untuk menghindari penerimaan pegawai yang memiliki rekam jejak yang kurang baik.	Proses pengecekan latar belakang antara lain dengan pengecekan SLIK minimal 1 tahun sekali, pengecekan media sosial atau kunjungan ke tempat tinggal pegawai. Sejauh ini yang paling efektif adalah pengecekan SLIK. Karena dari SLIK dapat dilihat gaya hidup pegawai dan pinjaman yang dimiliki, seperti pinjol atau paylater yang berisiko.		Bank Sleman memiliki pedoman terkait WBS dan sudah di-share di portal ketentuan internal sehingga setiap pegawai dapat mengakses secara bebas. Pada saat sosialisasi di setiap unit kerja, Tim Anti Fraud juga menjelaskan terkait WBS. Kekurangannya pegawai masih kurang aware terkait WBS dan masih takut untuk mengungkap kecurangan ataupun fraud di unit kerjanya.		
Mrs Rizky Chitra (19 February 2026)						

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Mrs Rizky Chitra (22 December 2025)						
Mrs Rizky Chitra (19 February 2026)						

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Mrs Rizky Chitra (22 December 2025)			Rekam jejak pegawai dilakukan untuk semua calon pegawai. Apabila calon pegawai sudah pernah bekerja, maka dilakukan pengecekan ke perusahaan lama, cross check dengan bagian HRD apakah calon pegawai tersebut memiliki rekam jejak yang baik atau kurang baik di perusahaan sebelumnya. Selain itu saat ini sudah ada aplikasi SIPELAKU dari OJK sehingga bagian SDM bisa mengecek apakah calon pegawai tersebut pernah terlibat dalam tindakan fraud sebelumnya. Tujuannya untuk menghindari penerimaan pegawai yang memiliki rekam jejak yang kurang baik.		
Mrs Rizky Chitra (19 February 2026)					

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Mrs Rizky Chitra (22 December 2025					
Mrs Rizky Chitra (19 February 2026)					

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Mrs Rizky Chitra (22 December 2025)		Apabila tidak ada perubahan atau tidak diterapkan di unit terkait. Di Bank Sleman untuk setiap pelatihan wajib dilakukan pre-test dan post-test untuk mengukur keseriusan peserta pada saat mengikuti pelatihan.	Efektifitas selama pelatihan dapat dilihat dari nilai pre-test dan post-test peserta. Sedangkan efektifitas setelah pelatihan dapat dilihat dari jumlah fraud yang terjadi serta kesalahan-kesalahan dalam pelaksanaan pekerjaan.		Efektifitas selama pelatihan dapat dilihat dari nilai pre-test dan post-test peserta. Sedangkan efektifitas setelah pelatihan dapat dilihat dari jumlah fraud yang terjadi serta kesalahan-kesalahan dalam pelaksanaan pekerjaan.	
Mrs Rizky Chitra (19 February 2026)						

	I. Follow-Up Actions	i. Provisions Update	ii. Refreshment
Mrs Rizky Chitra (22 December 2025)	R : Bagaimana perencanaan pelatihan tahunan disusun? I : Berdasarkan risiko lalu evaluasi kinerja serta usulan dari setiap unit kerja.	Iya. Berdasarkan temuan fraud, dari tim SAF akan membahas terkait temuan tersebut dengan manajemen, evaluasi sistem. Apabila dirasa ada yang perlu diubah atau di-update maka tim SAF akan mengusulkan perubahan atau pembuatan regulasi serta usulan pengadaan pelatihan.	Iya. Berdasarkan temuan fraud, dari tim SAF akan membahas terkait temuan tersebut dengan manajemen, evaluasi sistem. Apabila dirasa ada yang perlu diubah atau di-update maka tim SAF akan mengusulkan perubahan atau pembuatan regulasi serta usulan pengadaan pelatihan.
Mrs Rizky Chitra (19 February 2026)			

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Mr Dwi Handoyo Miharjo (9 December 2025)				Kalau whistleblower itu memang kita ada namanya Tim Anti Fraud. Di Bank Sleman itu ada Tim Anti Fraud. Nah, Tim Anti Fraud itu lintas unit kerja. Lintas unit kerja. Nah, yang mengelola whistleblower itu nanti memang ditunjuk adalah dari unit SDM. Pemilihannya ya? Kalau pemilihannya tidak ada mekanisme, cuman kita akan melibatkan unit-unit yang memang dirasa berwenang untuk mengurus hal tersebut. Karena kalau pakai mekanisme, takutnya unit yang tidak ada kaitannya malah bisa masuk dalam Tim Anti Fraud itu. Contoh, unit umum masuk Tim Anti Fraud, ya mungkin bisa aja, tapi dia tidak berkompeten di situ. Sehingga unit yang berkompeten seperti apa? Contoh tim audit, Satuan Kerja Audit Internal, Satuan Kerja Manajemen Risiko, kemudian SDM yang mengelola ini, dan Compliance. Jadi unit-unit yang terkait lah, unit-unit yang mungkin kira-kira memang akan berurusan dengan fraud. Timnya itu seluruh unit kerjanya. Misalnya di saya ada 3 orang, yaudah 3 orang itu masuk sebagai Tim Anti Fraud. jadi beda-beda ya memang tugasnya. Kalau Management Risk itu bertugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatormya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.	Oh ya, tentu. Jadi kalau fraud digital, karena divisi saya kan risk management ya. Departemen Compliance atau Kepatuhan. Saya jadi unit risk management. Lima tahu saya di risk management, kita otomatis setiap satu tahun, satu kali itu akan ada pelatihan terkait dengan fraud. Every fraud. Jadi bukan cuma fraud terkait dengan uang, tapi fraud bagaimana pembocoran data, rahasia data, dan lain-lain. Khusus SDMnya Management Risk ya? Jadi khusus departemen Management Risk, kita memang dibekali ya oleh SDM dan oleh perusahaan, jadi yang pertama kita pasti akan selalu diikutkan pelatihan-pelatihan yang berbau fraud, kemudian berbau audit, kemudian berbau terkait dengan compliance atau kepatuhan, jadi kemudian juga ada namanya APU-PPT, nah itu ita diikutkan pelatihan itu secara rutin secara konsep. Tujuannya apa? Tujuannya untuk meningkatkan kompetensi dari pegawai itu sendiri. Oh iya, kalau efektif, efektif, itu sangat membantu, karena ada hal-hal yang memang kita tidak bisa, misalnya kita belum tahu jadi tahu, atau mungkin ada aplikasi yang belum kita gunakan, di pelatihan tersebut ada penawaran aplikasi yang bermanfaat bagi kita, itu kita gunakan. Jadi itu sangat efektif.		Oke, yang paling relevan sebenarnya potensi risiko itu kapan saja bisa datang ya. Secara risiko fraud itu sebenarnya ada dua, ada dua poin. Yang pertama adalah human error dan system error. Kalau menurut saya cuma dua itu. Nah, kalau human error artinya kan fraud itu terjadi karena kompetensi si human-nya, si manusianya. Entah itu dia tidak mengetahui, oh ternyata saya melanggar dan it merugikan pihak bank, itu bisa jadi memang penyalahgunaan dan ketika orang tersebut mendapatkan keuntungan secara pribadi, itu bisa kita katakan fraud. jadi beda-beda ya memang tugasnya. Kalau Management Risk itu bertugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatormya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Mr Dwi Handoyo Miharjo (9 December 2025)		Selain itu, kita juga bukan hanya mendapatkan edukasi, kita juga memberikan edukasi ke unit kerja lainnya atau departemen lainnya. Di departemen saya, kebetulan itu, juga turut menyampaikan atau mensosialisasikan terkait dengan fraud prevention. Artinya, pencegahan fraud ya. Nah itu yang kita pengen, apa, tujuannya adalah kita pengen untuk teman-teman itu bisa sadar risiko sejak dini. Karena kebanyakan kan, orang-orang tau fraud itu, oke saya nyuri uang, saya mengatakan itu fraud. Tapi, fraud kan bukan cuma itu saja. Mungkin nanti mbak juga bisa mencari jawabannya, fraud itu apa saja. Tapi, misalnya kamu pembocoran rahasia, ada benturan kepentingan, itu sudah merencanakan ke area fraud. Jadi, itu menurut saya penting diketahui oleh seluruh unit kerja, bukan cuma unit saya sendiri. Oke, yang paling relevan sebenarnya potensi risiko itu kapan saja bisa datang ya. Secara risiko fraud itu sebenarnya ada dua, ada dua poin. Yang pertama adalah human error dan system error. Kalau menurut saya cuma dua itu. Nah, kalau human error artinya kan fraud itu terjadi karena kompetensi si human-nya, si manusianya. Entah itu dia tidak mengetahui, oh ternyata saya melanggar dan itu merugikan pihak bank, itu bisa jadi memang penyalahgunaan dan ketika orang tersebut mendapatkan keuntungan secara pribadi, itu bisa kita katakan fraud. Ya, jadi kalau untuk meningkatkan kesadaran dari anti fraud, kita setiap bulan itu melakukan kunjungan ya, kunjungan ke seluruh departemen untuk mensosialisasikan terkait dengan fraud prevention. Nah disitu kita jelaskan termasuk tadi whistleblowing dan lain-lain, itu kita jelaskan di setiap bulan itu di unit kerja berbeda masing-masing. Kenapa kita tidak kumpulkan dalam satu ruangan secara bersama-sama? Karena kami pengen lebih dekat sama per unit kerjanya. Saya rasa itu lebih efektif. Yang kedua memang secara umum, itu setiap tahun sudah ada terkait dengan fraud, sosialisasi juga. Selain itu kita juga ada yang namanya tanda tangan pakta integritas atau tanda tangan anti fraud untuk jadi beda-beda ya memang tugasnya. Kalau Management Risk itu tugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatornya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.	Ya, jadi kalau untuk meningkatkan kesadaran dari anti fraud, kita setiap bulan itu melakukan kunjungan ya, kunjungan ke seluruh departemen untuk mensosialisasikan terkait dengan fraud prevention. Nah disitu kita jelaskan termasuk tadi whistleblowing dan lain-lain, itu kita jelaskan di setiap bulan itu di unit kerja berbeda masing-masing. Kenapa kita tidak kumpulkan dalam satu ruangan secara bersama-sama? Karena kami pengen lebih dekat sama per unit kerjanya. Saya rasa itu lebih efektif. Yang kedua memang secara umum, itu setiap tahun sudah ada terkait dengan fraud, sosialisasi juga. Selain itu kita juga ada yang namanya tanda tangan pakta integritas atau tanda tangan anti fraud untuk		Kemudian di sisi lain, kita juga punya namanya FDS. FDS itu Fraud Detection System. Jadi, Fraud Detection System ini berfungsi untuk menganalisa atau menetapkan hal-hal yang di luar batas normal. Jadi itu parameterized ya, jadi itu ada parameternya. Parameternya itu misalnya seperti, oh ada transaksi ATM dilakukan secara bersamaan di selang waktu bersamaan, gitu. Jadi, itu FDS kita ngebaca itu, sistem kita ngebaca itu. Atau misalnya ada bukan nasabah tapi berhasil melakukan transaksi seperti itu. Atau ada rekening pasif tapi dapat melakukan transaksi. Jadi hal-hal yang tidak normal itu akan diketahui oleh FDS namanya, Fraud Detection System. Oke, langkah-langkahnya ya. Yang pertama kita ada beberapa langkah. Satu itu adalah kita punya namanya whistleblower. Whistleblower itu apa, jadi rekan-rekan kerja kita yang mengetahui indikasi fraud dengan bukti awal, itu kita mempersilahkan melaporkan ke unit kerja yang telah ditunjuk. Otomatis kerahasiaannya dari pegawai tersebut akan kami jamin seribu persen. Oke, kemudian nanti ada timnya tersendiri ketika laporannya sudah masuk, nanti akan ada tim investigation yang akan mengurus hal tersebut. Nah, yang kedua bagaimana kalau misalnya terjadi fraud, tadi kan saya bilang ada FDS ya, Fraud Detection System. Nah, ketika ada hal-hal indikasi, wah ternyata ada hal-hal yang nggak wajar nih, nah itu kita lakukan analisa juga. Itu tidak perlu pakai whistleblower, karena pihak eksternalnya. Jadi, kita menganalisa kalau misalnya memang ada hal-hal dirasa mencurigakan, kita akan melakukan prosedur-prosedur yang telah ditetapkan. Jadi ada sih mbak, hal-hal yang memang kita itu sudah punya prosedur untuk bagaimana sih kalau misalnya indikasi fraud-nya itu muncul atau misalnya ada terjadi fraud. Nah, di sisi lain kita juga kan di bawah regulator OJK dan BI. Nah, kalau untuk OJK itu juga kita punya kewajiban untuk melaporkan seluruh kejadian fraud dan itu secara rutin. Walaupun di periode tersebut tidak ada kejadian fraud, kita harus tetap melaporkan pelaporan anti fraud secara nihil karena memang tidak ada, tapi pelaporannya harus tetap jalan. Nah, di BI pun seperti itu Untuk Fraud Detection System ketika dilakukan analisa dan itu memang benar terjadi kecurangan, nah itu memang kita akan langsung sampaikan ke audit. Tapi kalau misalnya tidak, artinya stop sampai di SKMR saja. Sampai di Management Risk saja.	Risk register? Oke, mantap nih pertanyaan nya. Jadi risk register kita diperbarui, jadi setiap bulan kita, teman-teman itu mengisi risk register yang ada di seluruh unit kerja, mereka setiap bulan mengisi, meskipun memang ada beberapa unit kerja itu kadang kelewat ya mengisinya a, cuman tetap mengisi secsra bulanan.	Oke, kalau proses scoring itu kita mengikuti ketentuan POJK ya. Jadi, ada ketentuannya a POJK, POJK SE OJK nomor 1 tahun 2019. Itu adalah scoring terkait dengan profil risiko bank. Nah, itu nanti mbak bisa melihat di sana itu tata cara scoring itu sesuai regulator. Jadi, kita nggak bisa scoring asal scoring aja. Semuanya itu telah ditetapkan oleh POJK.	

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Mr Dwi Handoyo Miharjo (9 December 2025)			Kalau sering mungkin tidak juga, ya mungkin 3 tahun, 4 tahun. Saya sendiri 5 tahun di sana belum pindah ya. Tapi, bos saya sudah 2 kali pindah. Kemudian juga ada tim baru lagi. Jadi, saya rasa mungkin belum ya. Maksudnya belum-belum ada rotasi yang setiap tahun harus rotasi. Karena memang Management Risk tidak boleh terlalu banyak rotasi. Kenapa? Karena itu harus orang yang punya integritas yang baik, pemahaman perbankan yang baik, kemudian struktur dan cara berpikir yang baik.	Oke, langkah-langkahnya ya. Yang pertama kita ada beberapa langkah. Satu itu adalah kita punya namanya whistleblower. Whistleblower itu apa, jadi rekan-rekan kerja kita yang mengetahui indikasi fraud dengan bukti awal, itu kita mempersilahkan melaporkan ke unit kerja yang telah ditunjuk. Otomatis kerahasiaannya dari pegawai tersebut akan kami jamin seribu persen. Oke, kemudian nanti ada timnya tersendiri ketika laporannya sudah masuk, nanti akan ada tim investigation yang akan mengurus hal tersebut. Nah, yang kedua bagaimana kalau misalnya terjadi fraud, tadi kan saya bilang ada FDS ya, Fraud Detection System. Nah, ketika ada hal-hal indikasi, wah ternyata ada hal-hal yang nggak wajar nih, nah itu kita lakukan analisa juga. Itu tidak perlu pakai whistleblower, karena pihak eksternalnya. Jadi, kita menganalisa kalau misalnya memang ada hal-hal dirasa mencurigakan, kita akan melakukan prosedur-prosedur yang telah ditetapkan. Jadi ada sih mbak, hal-hal yang memang kita itu sudah punya prosedur untuk bagaimana sih kalau misalnya indikasi fraud-nya itu muncul atau misalnya ada terjadi fraud. Nah, di sisi lain kita juga kan di bawah regulator OJK dan BI. Nah, kalau untuk OJK itu juga kita punya kewajiban untuk melaporkan seluruh kejadian fraud dan itu secara rutin. Walaupun di periode tersebut tidak ada kejadian fraud, kita harus tetap melaporkan pelaporan anti fraud secara nihil karena memang tidak ada, tapi pelaporannya harus tetap jalan. Nah, di BI pun seperti itu. Kalau whistleblower itu memang kita ada namanya Tim Anti Fraud. Di Bank Sleman itu ada Tim Anti Fraud. Nah, Tim Anti Fraud itu lintas unit kerja. Lintas unit kerja. Nah, yang mengelola whistleblower itu nanti memang ditunjuk adalah dari unit SDM. Ya, jadi kalau untuk meningkatkan kesadaran dari anti fraud, kita setiap bulan itu melakukan kunjungan ya, kunjungan ke seluruh departemen untuk mensosialisasikan terkait dengan fraud prevention. Nah disitu kita jelaskan termasuk tadi whistleblowing dan lain-lain, itu kita jelaskan di setiap bulan itu di unit kerja berbeda masing-masing. Kenapa kita tidak kumpulkan dalam satu ruangan secara bersama-sama? Karena kami pengen lebih dekat sama per unit kerjanya. Saya rasa itu lebih efektif. Yang kedua memang secara umum, itu setiap tahun sudah ada terkait dengan fraud, sosialisasi juga. Selain itu kita juga ada yang namanya tanda tangan pakta integritas atau tanda tangan anti fraud untuk jadi beda-beda ya memang tugasnya. Kalau Management Risk itu tugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatornya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.		

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Mr Dwi Handoyo Miharjo (9 December 2025)						Oke, jadi kalau untuk fraud, tentu kita dari core banking itu sudah ada parameter-parameternya, red flag-nya juga sudah ada. Kemudian kita juga punya audit trail-nya ya. Jadi, kita melihat sistem ini digunakan oleh siapa saja, yang mengakses sistem itu siapa saja, sehingga ada transaksi-transaksi atau yang masuk ke dalam sistem yang mencurigakan itu bisa diketahui.

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Mr Dwi Handoyo Miharjo (9 December 2025)	Oke, jadi kalau untuk fraud, tentu kita dari core banking itu sudah ada parameter-parameternya, red flag-nya juga sudah ada. Kemudian kita juga punya audit trail-nya ya. Jadi, kita melihat sistem ini digunakan oleh siapa saja, yang mengakses sistem itu siapa saja, sehingga ada transaksi-transaksi atau yang masuk ke dalam sistem yang mencurigakan itu bisa diketahui. Oke, pertama kita meng-create parameter-parameter yang tidak bisa diakses oleh pegawai umum. Jadi, hanya pegawai-pegawai tertentu aja yang berwenang boleh masuk di sistem tersebut. Kemudian kalau ada kesalahan, sistem kita sudah men-detect lebih awal. Kemudian juga pengawasan melekat, baik itu secara offline yang misalnya target paraf, tanda tangan dan lain-lain itu semua ter-record. Jadi, pengawasan melekatnya itu terinventarisir dengan baik. Nah, itu yang membuat, seharusnya membuat orang-orang ketika melakukan fraud itu sulit untuk melakukan. Jadi, kita membuat sistem struktur organisasi yang flow-nya itu lengkap untuk meminimalisir potensi-potensi teman-teman melakukan kecurangan.		Jadi Alhamdulillah, fraud di kita itu kan memang sangat jarang terjadi ya. Kontrol kita kemungkinan besar kalaupun itu terjadi, artinya itu dari human-nya memang. Human-nya artinya mungkin dari apa? Mungkin dari kontrol kita yang kurang. Nah, itu yang kita selalu benahi. Jadi memang benar apa yang mbak sampaikan, pengawasan melekat, ketentuan, kontrol internal, sistem kontrol, itu yang menjadi pintu pencegahan kita untuk mengantisipasi terjadinya fraud itu. Oke, pertama kita meng-create parameter-parameter yang tidak bisa diakses oleh pegawai umum. Jadi, hanya pegawai-pegawai tertentu aja yang berwenang boleh masuk di sistem tersebut. Kemudian kalau ada kesalahan, sistem kita sudah men-detect lebih awal. Kemudian juga pengawasan melekat, baik itu secara offline yang misalnya target paraf, tanda tangan dan lain-lain itu semua ter-record. Jadi, pengawasan melekatnya itu terinventarisir dengan baik. Nah, itu yang membuat, seharusnya membuat orang-orang ketika melakukan fraud itu sulit untuk melakukan. Jadi, kita membuat sistem struktur organisasi yang flow-nya itu lengkap untuk meminimalisir potensi-potensi teman-teman melakukan kecurangan.	Oke, pertama kita meng-create parameter-parameter yang tidak bisa diakses oleh pegawai umum. Jadi, hanya pegawai-pegawai tertentu aja yang berwenang boleh masuk di sistem tersebut. Kemudian kalau ada kesalahan, sistem kita sudah men-detect lebih awal. Kemudian juga pengawasan melekat, baik itu secara offline yang misalnya target paraf, tanda tangan dan lain-lain itu semua ter-record. Jadi, pengawasan melekatnya itu terinventarisir dengan baik. Nah, itu yang membuat, seharusnya membuat orang-orang ketika melakukan fraud itu sulit untuk melakukan. Jadi, kita membuat sistem struktur organisasi yang flow-nya itu lengkap untuk meminimalisir potensi-potensi teman-teman melakukan kecurangan.	Oke, langkah-langkahnya ya. Yang pertama kita ada beberapa langkah. Satu itu adalah kita punya namanya whistleblower. Whistleblower itu apa, jadi rekan-rekan kerja kita yang mengetahui indikasi fraud dengan bukti awal, itu kita mempersilahkan melaporkan ke unit kerja yang telah ditunjuk. Otomatis kerahasiaannya dari pegawai tersebut akan kami jamin seribu persen. Oke, kemudian nanti ada timnya tersendiri ketika laporannya sudah masuk, nanti akan ada tim investigation yang akan mengurus hal tersebut. Nah, yang kedua bagaimana kalau misalnya terjadi fraud, tadi kan saya bilang ada FDS ya, Fraud Detection System. Nah, ketika ada hal-hal indikasi, wah ternyata ada hal-hal yang nggak wajar nih, nah itu kita lakukan analisa juga. Itu tidak perlu pakai whistleblower, karena pihak eksternalnya. Jadi, kita menganalisa kalau misalnya memang ada hal-hal dirasa mencurigakan, kita akan melakukan prosedur-prosedur yang telah ditetapkan. Jadi ada sih mbak, hal-hal yang memang kita itu sudah punya prosedur untuk bagaimana sih kalau misalnya indikasi fraud-nya itu muncul atau misalnya ada terjadi fraud. Nah, di sisi lain kita juga kan di bawah regulator OJK dan BI. Nah, kalau untuk OJK itu juga kita punya kewajiban untuk melaporkan seluruh kejadian fraud dan itu secara rutin. Walaupun di periode tersebut tidak ada kejadian fraud, kita harus tetap melaporkan pelaporan anti fraud secara nihil karena memang tidak ada, tapi pelaporannya harus tetap jalan. Nah, di BI pun seperti itu

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Mr Dwi Handoyo Miharjo (9 December 2025)	jadi beda-beda ya memang tugasnya. Kalau Management Risk itu bertugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatornya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.				Oke, langkah-langkahnya ya. Yang pertama kita ada beberapa langkah. Satu itu adalah kita punya namanya whistleblower. Whistleblower itu apa, jadi rekan-rekan kerja kita yang mengetahui indikasi fraud dengan bukti awal, itu kita mempersilahkan melaporkan ke unit kerja yang telah ditunjuk. Otomatis kerahasiaannya dari pegawai tersebut akan kami jamin seribu persen. Oke, kemudian nanti ada timnya tersendiri ketika laporannya sudah masuk, nanti akan ada tim investigation yang akan mengurus hal tersebut. Nah, yang kedua bagaimana kalau misalnya terjadi fraud, tadi kan saya bilang ada FDS ya, Fraud Detection System. Nah, ketika ada hal-hal indikasi, wah ternyata ada hal-hal yang nggak wajar nih, nah itu kita lakukan analisa juga. Itu tidak perlu pakai whistleblower, karena pihak eksternalnya. Jadi, kita menganalisa kalau misalnya memang ada hal-hal dirasa mencurigakan, kita akan melakukan prosedur-prosedur yang telah ditetapkan. Jadi ada sih mbak, hal-hal yang memang kita itu sudah punya prosedur untuk bagaimana sih kalau misalnya indikasi fraud-nya itu muncul atau misalnya ada terjadi fraud. Nah, di sisi lain kita juga kan di bawah regulator OJK dan BI. Nah, kalau untuk OJK itu juga kita punya kewajiban untuk melaporkan seluruh kejadian fraud dan itu secara rutin. Walaupun di periode tersebut tidak ada kejadian fraud, kita harus tetap melaporkan pelaporan anti fraud secara nihil karena memang tidak ada, tapi pelaporannya harus tetap jalan. Nah, di BI pun seperti itu

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Mr Dwi Handoyo Miharjo (9 December 2025)	jadi beda-beda ya memang tugasnya. Kalau Management Risk itu bertugasnya adalah prevention-nya. Jadi before-nya, before terjadi itu bagaimana kita sosialisasikan, bagaimana kita melakukan pencegahan, bagaimana kita mengedukasi teman-teman untuk fraud itu tidak boleh terjadi. Kemudian kalau Tim Audit itu dia sebagai investigatornya, investigasinya, dia melakukan analisa lebih dalam. Kemudian kalau SDM itu terkait dengan whistleblower-nya, nanti punishment-nya juga di ranah SDM. Kemudian kalau bagian kepatuhan atau Compliance itu nanti di ketentuannya. Apakah fraud ini terjadi karena kelemahan di ketentuan kita? Nah, jadi itu saling melengkapi.				Kalau untuk Anti Fraud itu nanti KPI-nya setahu saya bukan KPI atas nama Anti Fraud-nya, tapi KPI personalnya. Jadi KPI-nya itu lebih ke arah misalnya SKMR secara personal, KPI-nya sudah bagus, mengantisipasi hal-hal terjadinya fraud. Oh, Audit telah melakukan investigasi. Jadi per unit kerjanya ya, bukan Tim Anti Fraud-nya. Nah, untuk yang melakukan fraud-pun pasti tentu ada KPI-nya juga. Misalnya kamu melakukan fraud, otomatis KPI-mu akan turun. R : Berarti per individual begitu ya, Pak? I : Yes, betul.	

	1. Follow-Up Actions			i. Provisions Update		ii. Refreshment	
Mr Dwi Handoyo Miharjo (9 December 2025)							

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Mr Dwi Handoyo Miharjo (2 February 2026)							

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Mr Dwi Handoyo Miharjo (2 February 2026)		Oke, tentu kita selalu optimis bahwa kita inginnya strategi anti-fraud di Bank Sleman itu berjalan efektif terus mungkin sekarang juga bukan cuman sekedar efektif. Tapi anti-fraud juga memerlukan sebuah inovasi, sebuah sistem. Kemudian sebuah kebersamaan. Kebersamaan yang saya maksud adalah bagaimana culture terkait dengan anti-fraud, bukan dipahami oleh orang-orang risk saja, tapi oleh seluruh unit kerja, oleh seluruh pegawai bahkan oleh seluruh pekerja yang non-pegawai juga. Misalnya entah itu yang mungkin dari OB, mungkin dari satuan keamanan, dan lain-lain. Saya rasa pemahaman anti-fraud itu seluruhnya wajib dipahami oleh insan perbankan dari golongan apapun. Dan itu yang kita lakukan. Kita melakukan sosialisasi anti-fraud itu bukan cuman hanya ke bawah, bahkan sampai level tertentu, misalnya OB tadi dan lain-lain Itu juga kita sampaikan juga bahwa terkait dengan pentingnya pemahaman anti-fraud.	Mungkin sekaligus saya akan membahas terkait dengan antisipasinya seperti apa. Nah, antisipasinya kita setiap tahun, bahkan baru bulan ini juga, bulan Januari 2026. Itu kami menyelenggarakan semacam penandatanganan pakta integritas. Kita ada penandatanganan pakta integritas, ada penandatanganan kode etik perbankan Ada juga deklarasi anti-fraud. Jadi ini dilakukan setiap 6 bulan sekali di perbankan kami.					

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Mr Dwi Handoyo Miharjo (2 February 2026)						

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Mr Dwi Handoyo Miharjo (2 February 2026)					Nah, kemudian seluruh sudut ruangan kita juga dilengkapi oleh CCTV. Nah, jadi CCTV tersebut juga akan melihat bagaimana kalau misalnya ada uang fisik itu ada yang selisih khususnya di teller. Nah, itu juga menjadi salah satu bukti autentik untuk melihat bagaimana proses atau kejadian event-event tertentu yang menyebabkan adanya kekurangan, selisih, dan lain-lain itu melalui CCTV. Dan itu sangat worth it, sangat bermanfaat. Jadi, selain tadi authorization, double check, dual control, pengawasan melekat, kemudian ada proses audit, ada proses identifikasi risiko. Saya rasa cukup banyak hal-hal yang selain dengan pemanfaatan FDS.	

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Mr Dwi Handoyo Miharjo (2 February 2026)	Kemudian yang kedua sistem juga itu bisa punya audit trail. Jadi audit trail itu bagaimana sistem ini akan mengetahui siapa saja yang mengakses sistem tersebut, jam berapa bisa mengakses, dan apa yang diakses, apa yang di-download. Jadi semua backend dari sistem tersebut terbaca oleh audit trail. Nah, itu hal-hal yang tidak diketahui oleh petugas, karena petugas tidak punya akses tersebut.	Nah, bagaimana kalau atasan dan anak buahnya itu melakukan... melakukan kerjasama untuk melakukan fraud? Makanya kita ada ketentuan rolling session. Jadi kita di pegawai itu ada sistem rollingan juga. Nah, itu berkala memang paling sering itu teller untuk dilakukan rolling. Kenapa? Karena teller yang langsung bersinggungan dengan nasabah. Kemudian ada juga terkait dengan proses cuti. Cuti itu kan sebenarnya kita juga bukan asal cuti. Tapi yang menggantikan itu sekaligus mengecek pekerjaan temannya. Jadi ini adalah beberapa sebagian kecil tahapan dari perusahaan untuk mengantisipasi adanya resiko-resiko potensi terjadinya fraud itu.	Nah, selain itu apalagi, selain itu kita memiliki pengawasan melekat yang dimana seluruh supervisor mengawasi secara langsung. Baik catatan, baik sistem, baik konfirmasi ke nasabah langsung. Jadi misalnya, yang penyaluran kredit tadi, ada kemungkinan dapat gratifikasi, kita akan me-check langsung ke nasabah. Kita akan melakukan konfirmasi juga ke nasabah, apakah dengan pelayanan petugas yang telah melakukan proses pencairan kredit. Nah, itu yang ke... itu bentuk pengawasan ya. Kemudian tadi, bagaimana mengatasi. Misalnya pick up service dan delivery service, itu kita juga ada pengawasan melekatnya. Supervisor turun tangan langsung. Nominalnya kita konfirmasi langsung juga ke nasabah pada saat penyetoran atau penarikan. Kemudian buku tabungannya juga kita cek secara langsung, dikonfirmasi oleh petugas. Jadi ketika ada kelalaian, itu seharusnya tidak bisa dilakukan oleh personality atau satu orang secara sistem. Nah, bagaimana kalau atasan dan anak buahnya itu melakukan... melakukan kerjasama untuk melakukan fraud? Makanya kita ada ketentuan rolling session. Jadi kita di pegawai itu ada sistem rollingan juga. Nah, itu berkala memang paling sering itu teller untuk dilakukan rolling. Kenapa? Karena teller yang langsung bersinggungan dengan nasabah. Kemudian ada juga terkait dengan proses cuti. Cuti itu kan sebenarnya kita juga bukan asal cuti. Tapi yang menggantikan itu sekaligus mengecek pekerjaan temannya. Jadi ini adalah beberapa sebagian kecil tahapan dari perusahaan untuk mengantisipasi adanya resiko-resiko potensi terjadinya fraud itu.	Oke, deteksi fraud, deteksi fraud, kalau misalnya kita bicara secara sistemnya. Itu selain FDS tentu kita ada otorisasi dan verifikasi. Jadi tidak semua pegawai itu melakukan single authorization. Nah, kita ada bertahap atau skala bertahap dalam melakukan otorisasi. Ketika salah satu petugas itu melakukan otorisasi tertentu, itu tidak bisa serta-merta otorisasi itu hanya di satu petugas tersebut, tapi ada tingkatannya juga, jadi ibaratnya kita ada dual control-nya seperti itu, atau double check-nya. Nah, itu yang pertama.	

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Mr Dwi Handoyo Miharjo (2 February 2026)				Oke, fraud secara signifikan dan tidak itu kita punya komitenya. Jadi kita ada komite, di mana komite tersebut itu memang dibentuk lintas unit kerja. Jadi ada namanya kita komite anti-fraud, jadi penentuan signifikansi dan tidak signifikannya suatu kejadian fraud. Itu ditentukan dari hasil pembicaraan dalam komite dan tim tersebut. Tentu kita akan menimbang kerugiannya. Kita akan menimbang besarnya kasus tersebut seperti apa. Dan ya alhamdulillah, setau saya saat ini tidak ada yang bersignifikan. Oke, kalau dibuat laporannya kita tetap akan membuat laporannya. Cuma sejauh mana kita akan membuktikan itu. Kadangkan kalau misalnya masih tahapan, kita kan ada tahapan-tahapannya ya. Kalau tahapannya masih di low-middle saya rasa sih kita masih belum membuat laporannya. Tapi kalau rasa-rasanya itu sudah menjelang benar-benar ada yang terdapat, terjadi. Meskipun ada kerugian tapi misalnya tidak menunjuk salah satu orang dan lain-lain. Nah itu kita buat laporannya.	Oke, kalau untuk beberapa tahun terakhir setahun saya, itu memang belum ada terjadi fraud yang secara signifikan. Dan itu memang, cuman memang kan kalau di OJK itu mau nihil itu tetap kita laporkan. Nah, jadi secara signifikan itu belum ada, alhamdulillah.

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Mr Dwi Handoyo Miharjo (2 February 2026)						

	I. Follow-Up Actions	i. Provisions Update	ii. Refreshment
Mr Dwi Handoyo Miharjo (2 February 2026)			

	RQ 2 Anti-Fraud Strategy Implementation	2. Strategy Implementation	a. Anti-Fraud Awareness	i. Anti-Fraud Team	ii. Anti-Fraud Training	iii. Competence Certification	iv. Regulations and Provisions Formulation
Mrs Dian Chandra Dewi (9 December 2025)				Iya, kalau sosialisasi untuk ketentuan internal fraud iya, tapi biasanya kita itu ada Tim Anti Fraud, disitu ada bagian Kepatuhan, kemudian ada bagian Manajemen Risiko, kemudian ada SDM, ada Internal Audit. Kita untuk melakukan sosialisasi itu memang bersama-sama ya untuk temanya, tapi untuk dalam penyampaian kebijakannya itu memang dari kepatuhan. Ya, karena dia ada petugas whistleblowing, jadi dia juga masuk	Ya, jadi untuk yang terkait fraud sendiri itu setiap tahun wajib dari POJK, jadi kita memang juga dari SDM kita sendiri itu harus mendapatkan pelatihan fraud. Kemudian kita juga harus melakukan pelatihan untuk kepatuhan, karena memang semua pegawai itu harus paham, jadi setiap tahun diulang gitu. Kalau pelatihan kan memang, kita terus ya, kita sosialisasikan, kemudian kita juga kasih contoh-contoh, mungkin sebenarnya yang paling, apa ya, mengenai itu ya kayak contoh-contoh itu, ya. Atau mungkin kalau ada terjadi fraud internal di Bank Sleman gitu kita bisa sampaikan dampaknya seperti apa agar lebih mengenai gitu. Karena real terjadi dan kita bisa lihat sendiri sekarang orangnya seperti apa keadaannya. Atau kita juga bisa sharing dengan bank-bank lain, kan itu banyak ya yang ada di internet, kita bisa ambil itu.		Jadi Internal Audit itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi ulang, refreshment. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan Internal Audit gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke Internal Audit supaya memang yang berhak untuk melakukan audit itu kan dari Internal Audit, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi. Iya pasti ya, karena kita Kepatuhan jadi kita memastikan adanya kebijakannya, kemudian kita pastikan juga ini sosialisasinya sudah dilakukan atau belum, kemudian apakah teman-teman itu memahami dari ketentuan anti fraud ini. Memang kita memastikan dulu ketentuan kita dulu ya, pas dalam kita membuat kebijakan anti fraud itu, kita lihat apakah sesuai POJK, SEOJK itu. Nah nanti untuk pelaksanaannya apakah sudah sesuai POJK atau belum, itu ketika ketentuan kita kan sudah tersesuaian dengan kewajiban POJK tadi, nah jadi seperti tadi, kalau memang dari SOP kita sudah sesuai nanti kita punya pelaksanaan yang kita sosialisasi lagi, kita ukur dari ada tidaknya fraud di tahun itu, kemudian ada post-test.
Mrs Dian Chandra Dewi (28 February 2026)							

	v. Anti-Fraud Publication	vi. Anti-Fraud Socialization	vii. Integrity Pact	b. Fraud Risk Identification	i. Fraud Detection System	ii. Risk Register	iii. Profile Risk Scoring	c. Know Your Employee
Mrs Dian Chandra Dewi (9 December 2025)	Upaya kesadaran terkait fraud, kita kan setiap bulan melakukan sosialisasi anti fraud, ke semua yang kerja, kita rolling setiap bulan. Kemudian juga di desktop-nya PC karyawan masing-masing, itu sudah kita tampilkan wallpaper-nya itu adalah anti fraud, misalkan jangan lakukan fraud, terus keluarga di rumah menunggu, kaya gitu. Kemudian kita juga di depan itu kan ada TV, di semua kantor cabang juga ada TV, di depan akses itu juga ada, kita juga buat dan tampilkan poster anti fraud. Kemudian kita juga kan di sosialisasi anti fraud itu, kita juga mau memberikan contoh-contoh fraud yang mungkin yang kita alami, jadi kasus-kasus fraud yang kita lihat proses hukumannya, itu kita juga sampaikan.	Jadi Internal Audit itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi ulang, refreshment. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan Internal Audit gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke Internal Audit supaya memang yang berhak untuk melakukan audit itu kan dari Internal Audit, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi. Iya pasti ya, karena kita Kepatuhan jadi kita memastikan adanya kebijakannya, kemudian kita pastikan juga ini sosialisasinya sudah dilakukan atau belum, kemudian apakah teman-teman itu memahami dari ketentuan anti fraud ini. Iya, kalau sosialisasi untuk ketentuan internal fraud iya, tapi biasanya kita itu ada Tim Anti Fraud, disitu ada bagian Kepatuhan, kemudian ada bagian Manajemen Risiko, kemudian ada SDM, ada Internal Audit. Kita untuk melakukan sosialisasi itu memang bersama-sama ya untuk temanya, tapi untuk dalam penyampaian kebijakannya itu memang dari kepatuhan. Kita bisa melihatnya memang dari ada tidaknya fraud ya di tahun itu. Nah, cuma kita juga ada, ketika sosialisasi itu kita kasih post-test, jadi di post-test itu kita menentukan nilainya dia lulus berapa, nah ketika semuanya lulus maka itu sudah jadi salah satu indikator kalau SOPnya itu sudah tersosialisasi. Memang kita memastikan dulu ketentuan kita dulu ya, pas dalam kita membuat kebijakan anti fraud itu, kita lihat apakah sesuai POJK, SEOJK itu. Nah nanti untuk pelaksanaannya apakah sudah sesuai POJK atau belum, itu ketika ketentuan kita kan sudah tersesuaikan dengan kewajiban POJK			Nah untuk fraud sendiri kalau untuk aplikasi digital ini terkait dengan transaksi ATM dan virtual account itu kita memang ada yang namanya sistemnya Fraud Detection System, FDS ya, terus dia nempel di aplikasinya itu, disitu kita buat parameternya apa sih yang kira-kira terkait fraud itu, misal dia transaksinya di ATM yang jangkauannya jauh dari Bank Sleman, kemudian transaksinya dua kali, di ATM yang berbeda dengan jarak yang jauh, itu kan bisa menjadi parameter terjadinya fraud kayak gitu, nah itu nanti akan masuk ke FDS, jadi di FDS itu nanti otomatis akan terblokir rekeningnya, nah baru setelah itu akan dilakukan cek dari bagian fraudnya, Anti Fraud, nanti akan dicek bahwa ini transaksinya apakah memang nasabah atau bukan, kalau memang bukan nasabah, nanti akan konsultasi juga sama nasabah apakah memang ini transaksi nasabah atau bukan, kalau memang itu transaksi nasabah, maka nasabah nanti bisa kesini dan bisa melakukan penggantian ATM, soalnya mungkin ATMnya itu kalau masuk ke red flag itu ya, ini tuh apakah kalau memang nasabahnya dia nanti bisa ganti ATM atau dia bisa buka blokirnya, tapi kalau misalkan itu bukan nasabah, ya dia harus langsung ganti ATMnya, karena mungkin sudah terkena orang, ter-hack gitu ya. itu memang kita sudah ada yang tadi ada FDS, kemudian itu juga sudah ada ketentuannya, parameternya sudah ditetapkan. Kemudian ada juga yang kita melakukan analisa transaksi tadi, yang kita menilai internetnya mencurigakan atau engga, itu di luar FDS ya. Kemudian ada juga untuk yang fraud internal, itu kita bisa melihat dari sistem itu juga, wajib terdapat audit trail. Jadi untuk semua yang masuk ke sistem, kita pasti ada user dan password, kita sudah melakukan juga untuk membuat ketentuan harus ada, untuk membalas sistem harus ada audit trail-nya, kemudian disitu harus bisa dilihat siapa yang terakhir kan mengakses, apa akses apa yang dia lakukan dan dia ubah			
Mrs Dian Chandra Dewi (28 February 2026)								

	i. Employee Recruitment	ii. Internal Employee	iii. Employee Turnover	d. Whistleblowing System	e. Surprise Audit	i. Planning
Mrs Dian Chandra Dewi (9 December 2025)				Kita ada melalui portal, melalui web Bank Sleman itu ada, untuk yang internal maupun eksternal. Misalkan pihak eksternal mau melaporkan tentang pelanggaran internal, pelanggaran pegawai Bank Sleman, itu bisa juga di web tersebut. Dan kita sebenarnya sudah secara aktif melakukan itu, kalau internal itu kita juga bisa melalui sistem whistleblowing, atau melalui langsung ke petugas whistleblowing nya. Jadi bisa langsung, misalkan memang tidak mau secara tertulis, dia maunya bertemu langsung, misalkan ke petugas whistleblowing itu juga bisa. Petugasnya itu ada di bagian SDM. Mekanismenya memang dari laporan itu, nanti dari SDM sebagai whistleblowing officer tadi, dia akan melakukan deteksi dulu, dia menginvestigasi dulu, ini memang ada buktinya atau tidak. Ketika memang ada buktinya, itu akan ditindaklanjuti melalui Internal Audit, jadi mungkin SDM yang menyampaikan ke Internal Audit untuk dilakukan investigasi. Kemudian dari Internal Audit, nanti akan melakukan investigasi fraudnya itu, dan akan menyatakan hasilnya nanti ke SDM. Jadi hasilnya itu memang fraud atau bukan. Atau mungkin bukan fraud namun pelanggaran ketentuan, pelanggaran ketentuan internal, tidak ada yang dirugikan, seperti itu misalnya. Nah, nanti dari SDM menarik hasil investigasi itu, kemudian akan melakukan rapat komite SDM, jadi yang berhak menentukan sanksinya itu dari komite SDM. Nah, ini memang fraud atau bukan, dan kemudian sanksinya apa yang akan diberikan. Kendalanya itu adalah ketika ada pelaporannya, tapi tidak terdapat buktinya. Jadi SDM harus mencari dulu, ini apakah memang betul atau tidak. Nah, kemudian kalau memang tidak ada buktinya, kemudian itu cuma kayak gosip atau apa, itu kan tidak bisa ditindaklanjuti. Tapi dari kendala yang di web itu, itu memang juga belum sempurna ya, karena harusnya kan dia bukan satu form yang harus di-download, kemudian di-scan, habis itu di-upload, itu kan agak menyulitkan sebenarnya untuk whistleblower ya. Nah, itu kendalanya juga di situ, jadi kita sebenarnya mau merubah itu jadi langsung inputan, langsung masuk ke whistleblowing officer. Tapi memang untuk pengembangan itu harus membutuhkan waktu, jadi untuk sementara kita menggunakan itu. Cuma ya itu tadi kendalanya harus di-print dulu, harus diisi, harus di-upload, kayak gitu. Terus kendalanya itu juga ada kalau untuk, kadang kan orang takut juga ya untuk melaporkan gitu ya, mungkin kalau bawahan untuk melaporkan atasannya kayak gitu kan, walaupun sebenarnya aman, kita sudah mensosialisasikan juga, tapi kadang memang masih ada takut di-blacklist, kadang-kadang itu jadi juga kendala whistleblowing, walaupun sebenarnya sudah tanpa nama seperti itu, cuman ya itu juga masih menjadi kendala, jadi kayak angkanya whistleblowing itu masih rendah. Tentang perlindungannya, ya tadi perlindungan dari identitas menjadi rahasia, identitas whistleblower. Kemudian apabila masuk ke pengadilan, nah itu nanti akan diberikan fasilitas sesuai kayak fasilitas konsultan hukum		Nah itu semua unit kerja itu sudah ditetapkan pas di awal tahun itu sudah ada rencana auditnya, jadi sudah ditetapkan nanti audit ini kapan. Tapi ada juga kalau misalkan terjadi fraud, nah itu langsung dilakukan audit seketika.
Mrs Dian Chandra Dewi (28 February 2026)						

	ii. Inspection	iii. Cash Opname	iv. External Audit	f. Surveillance System	i. CCTV	ii. Red Flag Check
Mrs Dian Chandra Dewi (9 December 2025)	Yang melakukan audit itu kan memang dari Internal Audit ya, kalau unit kerjanya itu ditentukan memang semua unit kerja itu memang diaudit, nah cuma nanti kan di pas pelaksanaan auditnya itu on the spot saja.			Surveillance system itu sebenarnya kita lakukan juga, nah itu kalau kewenangannya dari IT, kalau kita juga melakukan itu, sebenarnya setahun sekali ya kita lakukan.		Nah untuk fraud sendiri kalau untuk aplikasi digital ini terkait dengan transaksi ATM dan virtual account itu kita memang ada yang namanya sistemnya Fraud Detection System, FDS ya, terus dia nempel di aplikasinya itu, disitu kita buat parameternya apa sih yang kira-kira terkait fraud itu, misal dia transaksinya di ATM yang jangkauannya jauh dari Bank Sleman, kemudian transaksinya dua kali, di ATM yang berbeda dengan jarak yang jauh, itu kan bisa menjadi parameter terjadinya fraud kayak gitu, nah itu nanti akan masuk ke FDS, jadi di FDS itu nanti otomatis akan terblokir rekeningnya, nah baru setelah itu akan dilakukan cek dari bagian fraudnya, Anti Fraud, nanti akan dicek bahwa ini transaksinya apakah memang nasabah atau bukan, kalau memang bukan nasabah, nanti akan konsultasi juga sama nasabah apakah memang ini transaksi nasabah atau bukan, kalau memang itu transaksi nasabah, maka nasabah nanti bisa kesini dan bisa melakukan penggantian ATM, soalnya mungkin ATMnya itu kalau masuk ke red flag itu ya, ini tuh apakah kalau memang nasabahnya dia nanti bisa ganti ATM atau dia bisa buka blokirnya, tapi kalau misalkan itu bukan nasabah, ya dia harus langsung ganti ATMnya, karena mungkin sudah terkena orang, ter-hack gitu ya.
Mrs Dian Chandra Dewi (28 February 2026)						

	iii. Audit Trail	iv. Job Desc Check	v. Attached Supervision	vi. Authorization	g. Investigation
Mrs Dian Chandra Dewi (9 December 2025)	Kemudian ada juga untuk yang fraud internal, itu kita bisa melihat dari sistem itu juga, wajib terdapat audit trail. Jadi untuk semua yang masuk ke sistem, kita pasti ada user dan password, kita sudah melakukan juga untuk membuat ketentuan harus ada, untuk membalas sistem harus ada audit trail-nya, kemudian disitu harus bisa dilihat siapa yang terakhir kan mengakses, apa akses apa yang dia lakukan dan dia ubah.		Nah, ini kalau kita juga melakukan pengawasan itu dari banyaknya pertanyaan. Jadi kita karena Kepatuhan itu juga mempunyai tugas memberikan konsultasi ke unit kerja, jadi ketika unit kerja itu berkonsultasi ke kita, kita itu akan mencatat. Jadi nanti dari pertanyaan itu kita lihat berapa banyak sih pertanyaan yang sama yang dilontarkan dari unit-unit kerja itu, berapa kali, misalnya pertanyaannya tentang poin ketentuan itu sudah ada 5 pertanyaan, dan itu sama semua, berarti mungkin dia butuh dilakukan refreshment. Atau mungkin ada pertanyaan-pertanyaan yang memang membutuhkan review kebijakan, ternyata pada pelaksanaan yang tidak bisa, nah itu kita lakukan review kebijakan. Terus di Kepatuhan juga kita sebenarnya melakukan analisa transaksi, ini untuk APU-PPT, itu untuk anti pencucian uang itu bisa dijadikan fraud juga ya sebenarnya, fraud dari pihak eksternal gitu, nah kita juga melakukan analisa transaksi itu pakai sistem setiap bulan. Kalau anti fraud, menurut saya yang paling rentan itu bagian yang memegang uang, kayak funding, lending, kredit, kemudian bagian teller. Bukan Cuma di Bank Sleman namun di bank lainpun juga memang di bagian itulah yang rentan terjadi fraud. Karena memang setiap hari berurusan dengan nasabah, sudah tahu karakteristik nasabah, jadi setiap hari tanggung jawabnya memang mengelola dana nasabah. Jadi yang bagian yang paling rentan itu adalah itu, dan kita tanggulangnya dengan memang kita di bagian-bagian itu kita sudah buat sistemnya. Misalkan dia mau backup dana nasabah, dia harus mencatat dulu, kemudian dia harus izin dulu ke atasannya, mau apa nasabah mana aja backup-nya, kemudian setelah selesai nanti nominalnya berapa yang dia ambil. Kemudian ketika dia akan melakukan di teller untuk transaksi, itu teller-nya juga melakukan konfirmasi, benar atau tidak, mau melakukan penarikan sebesar ini, atau benar atau tidak, buat transaksi setoran nominalnya sekian melalui akun ini. Untuk transaksi teller juga, mereka untuk transaksi nominal tertentu, mungkin kalau di kita itu sekitar 15 juta, itu harus ada approve dari atasannya, mau dia penarikan atau setoran, kemudian ada juga untuk rekeningnya, yang sudah lama tidak bertransaksi, kadang ada rekening yang memang nasabah menabung satu miliar misalnya, dan itu memang dia mau disimpan buat investasi, jadi nggak pernah ditarik atau apa, itu kan kita juga ada sistemnya langsung sebagai rekening pasif, jadi dia tidak bisa melakukan transaksi, memang nasabahnya	itu memang kita sudah ada yang tadi ada FDS, kemudian itu juga sudah ada ketentuannya, parameternya sudah ditetapkan. Kemudian ada juga yang kita melakukan analisa transaksi tadi, yang kita menilai internetnya mencurigakan atau engga, itu di luar FDS ya. Kemudian ada juga untuk yang fraud internal, itu kita bisa melihat dari sistem itu juga, wajib terdapat audit trail. Jadi untuk semua yang masuk ke sistem, kita pasti ada user dan password, kita sudah melakukan juga untuk membuat ketentuan harus ada, untuk membalas sistem harus ada audit trail-nya, kemudian disitu harus bisa dilihat siapa yang terakhir kan mengakses, apa akses apa yang dia lakukan dan dia ubah	
Mrs Dian Chandra Dewi (28 February 2026)					

	i. Assignment to Authorized Parties	ii. Collecting Evidence	h. Reporting	i. Internal Reporting	ii. External Reporting
Mrs Dian Chandra Dewi (9 December 2025)	Jadi Internal Audit itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi ulang, refreshment. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan Internal Audit gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke Internal Audit supaya memang yang berhak untuk melakukan audit itu kan dari Internal Audit, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi.	Mekanismenya memang dari laporan itu, nanti dari SDM sebagai whistleblowing officer tadi, dia akan melakukan deteksi dulu, dia menginvestigasi dulu, ini memang ada buktinya atau tidak. Ketika memang ada buktinya, itu akan ditindaklanjuti melalui Internal Audit, jadi mungkin SDM yang menyampaikan ke Internal Audit untuk dilakukan investigasi. Kemudian dari Internal Audit, nanti akan melakukan investigasi fraudnya itu, dan akan menyatakan hasilnya nanti ke SDM. Jadi hasilnya itu memang fraud atau bukan. Atau mungkin bukan fraud namun pelanggaran ketentuan, pelanggaran ketentuan internal, tidak ada yang dirugikan, seperti itu misalnya. Nah, nanti dari SDM menarik hasil investigasi itu, kemudian akan melakukan rapat komite SDM, jadi yang berhak menentukan sanksinya itu dari komite SDM. Nah, ini memang fraud atau bukan, dan kemudian sanksinya apa yang akan diberikan.			
Mrs Dian Chandra Dewi (28 February 2026)					

	i. Punishment Imposition	j. Monitoring	i. Fraud Rate Tracking	k. Evaluation	i. KPI	ii. Penetration Test
Mrs Dian Chandra Dewi (9 December 2025)	Mekanismenya memang dari laporan itu, nanti dari SDM sebagai whistleblowing officer tadi, dia akan melakukan deteksi dulu, dia menginvestigasi dulu, ini memang ada buktinya atau tidak. Ketika memang ada buktinya, itu akan ditindaklanjuti melalui Internal Audit, jadi mungkin SDM yang menyampaikan ke Internal Audit untuk dilakukan investigasi. Kemudian dari Internal Audit, nanti akan melakukan investigasi fraudnya itu, dan akan menyatakan hasilnya nanti ke SDM. Jadi hasilnya itu memang fraud atau bukan. Atau mungkin bukan fraud namun pelanggaran ketentuan, pelanggaran ketentuan internal, tidak ada yang dirugikan, seperti itu misalnya. Nah, nanti dari SDM menarik hasil investigasi itu, kemudian akan melakukan rapat komite SDM, jadi yang berhak menentukan sanksinya itu dari komite SDM. Nah, ini memang fraud atau bukan, dan kemudian sanksinya apa yang akan diberikan.		Kita bisa melihatnya memang dari ada tidaknya fraud ya di tahun itu. Nah, cuma kita juga ada, ketika sosialisasi itu kita kasih post-test, jadi di post-test itu kita menentukan nilainya dia lulus berapa, nah ketika semuanya lulus maka itu sudah jadi salah satu indikator kalau SOPnya itu sudah tersosialisasi. Memang kita memastikan dulu ketentuan kita dulu ya, pas dalam kita membuat kebijakan anti fraud itu, kita lihat apakah sesuai POJK, SEOJK itu. Nah nanti untuk pelaksanaannya apakah sudah sesuai POJK atau belum, itu ketika ketentuan kita kan sudah tersesuaian dengan kewajiban POJK tadi, nah jadi seperti tadi, kalau memang dari SOP kita sudah sesuai nanti kita punya pelaksanaan yang kita sosialisasi lagi, kita ukur dari ada tidaknya fraud di tahun itu, kemudian ada post-test. Nah itu tadi seperti, kita kan setiap tahun akan melakukan penetration test. Kemudian kita juga lihat apa kejahatan-kejahatan yang ada. Kemudian kalau soal internal juga, kita lihat dalam satu tahun itu, apa sih temuan dari Internal Audit yang terkait dengan fraud, atau ada tidaknya fraud. Nah, ketika memang ada, kita bisa melihat kenapa bisa terjadi		Kita bisa melihatnya memang dari ada tidaknya fraud ya di tahun itu. Nah, cuma kita juga ada, ketika sosialisasi itu kita kasih post-test, jadi di post-test itu kita menentukan nilainya dia lulus berapa, nah ketika semuanya lulus maka itu sudah jadi salah satu indikator kalau SOPnya itu sudah tersosialisasi. Memang kita memastikan dulu ketentuan kita dulu ya, pas dalam kita membuat kebijakan anti fraud itu, kita lihat apakah sesuai POJK, SEOJK itu. Nah nanti untuk pelaksanaannya apakah sudah sesuai POJK atau belum, itu ketika ketentuan kita kan sudah tersesuaian dengan kewajiban POJK tadi, nah jadi seperti tadi, kalau memang dari SOP kita sudah sesuai nanti kita punya pelaksanaan yang kita sosialisasi lagi, kita ukur dari ada tidaknya fraud di tahun itu, kemudian ada post-test.	Nah itu tadi seperti, kita kan setiap tahun akan melakukan penetration test. Kemudian kita juga lihat apa kejahatan-kejahatan yang ada. Kemudian kalau soal internal juga, kita lihat dalam satu tahun itu, apa sih temuan dari Internal Audit yang terkait dengan fraud, atau ada tidaknya fraud. Nah, ketika memang ada, kita bisa melihat kenapa bisa terjadi fraud itu, jadi setiap tahun kita melakukan evaluasi tentang fraud.
Mrs Dian Chandra Dewi (28 February 2026)						

	i. Follow-Up Actions	ii. Provisions Update	iii. Refreshment
Mrs Dian Chandra Dewi (9 December 2025)		Jadi Internal Audit itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi ulang, refreshment. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan Internal Audit gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke Internal Audit supaya memang yang berhak untuk melakukan audit itu kan dari Internal Audit, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi. Untuk review peraturan kalau yang terkait fraud itu jika memang koordinasi sama Internal Audit kayak tadi, jadi dari hasil temuannya itu apa, nanti kita lihat kebutuhannya, kebutuhannya apakah kebijakannya itu perlu di-review, atau perlu di-refreshment lagi, atau perlu dirubah, seperti itu. Nah, ini kalau kita juga melakukan pengawasan itu dari banyaknya pertanyaan. Jadi kita karena Kepatuhan itu juga mempunyai tugas memberikan konsultasi ke unit kerja, jadi ketika unit kerja itu berkonsultasi ke kita, kita itu akan mencatat. Jadi nanti dari pertanyaan itu kita lihat berapa banyak sih pertanyaan yang sama yang dilontarkan dari unit-unit kerja itu, berapa kali, misalnya pertanyaannya tentang poin ketentuan itu sudah ada 5 pertanyaan, dan itu sama semua, berarti mungkin dia butuh dilakukan refreshment. Atau mungkin ada pertanyaan-pertanyaan yang memang membutuhkan review kebijakan, ternyata pada pelaksanaan yang tidak bisa, nah itu kita lakukan review kebijakan. Terus di Kepatuhan juga kita sebenarnya melakukan analisa transaksi, ini untuk APU-PPT, itu untuk anti pencucian uang itu bisa dijadikan fraud juga ya sebenarnya, fraud dari pihak eksternal gitu, nah kita juga melakukan analisa transaksi itu pakai sistem setiap bulan. Nah itu tadi seperti, kita kan setiap tahun akan melakukan penetration test. Kemudian kita juga lihat apa kejahatan-kejahatan yang ada. Kemudian kalau soal internal juga, kita lihat dalam satu tahun itu, apa sih temuan dari Internal Audit yang terkait dengan fraud, atau ada tidaknya fraud. Nah, ketika memang ada, kita bisa melihat kenapa bisa terjadi fraud itu, kekurangannya di ketentuan internal apa, jadi setiap tahun kita melakukan evaluasi tentang fraud.	Jadi Internal Audit itu kan menggunakan audit setelah terjadinya ada ketidakpatuhan, terjadinya pelanggaran. Nanti dari kepatuhan itu akan melakukan dari temuannya si audit itu kita akan melakukan, apa nih kebutuhan yang mungkin terjadi banyak pelanggaran di poin itu. Nah, kita akan memberikan sosialisasi ulang, refreshment. Kemudian apabila ada temuan yang berisiko, ternyata di unit kerja itu belum ada ketentuannya, jadi kita keluarkan ketentuannya seperti itu, dan kita juga melihat berapa banyak temuan terkait suatu ketentuan, misalnya memang temuannya itu banyak di poin itu terus, berarti mungkin poin itu memang harus ada kita lakukan penyesuaian. Mungkin memang sudah tidak sesuai dengan kondisi sekarang, perubahan, kan kita untuk kebijakan itu kan harus berkembang mengikuti zamannya, jadi mungkin memang itu sudah tidak sesuai. Kalau koordinasi antara Kepatuhan dan Internal Audit gitu, atau misalkan kita dari kepatuhan juga bisa, misalkan kita menemukan pelanggaran kepatuhan ya, kita bisa menyampaikan ke Internal Audit supaya memang yang berhak untuk melakukan audit itu kan dari Internal Audit, jadi misalkan kita tahu ada pelanggaran kepatuhan, kita bisa apa yang terjadi itu bisa dicek kembali soalnya kemana ada ketidakpatuhan ini, kemudian dia ternyata ketidakpatuhannya sudah terlalu jauh gitu ya, jadi itu ada koordinasi. Untuk review peraturan kalau yang terkait fraud itu jika memang koordinasi sama Internal Audit kayak tadi, jadi dari hasil temuannya itu apa, nanti kita lihat kebutuhannya, kebutuhannya apakah kebijakannya itu perlu di-review, atau perlu di-refreshment lagi, atau perlu dirubah, seperti itu. Nah, ini kalau kita juga melakukan pengawasan itu dari banyaknya pertanyaan. Jadi kita karena Kepatuhan itu juga mempunyai tugas memberikan konsultasi ke unit kerja, jadi ketika unit kerja itu berkonsultasi ke kita, kita itu akan mencatat. Jadi nanti dari pertanyaan itu kita lihat berapa banyak sih pertanyaan yang sama yang dilontarkan dari unit-unit kerja itu, berapa kali, misalnya pertanyaannya tentang poin ketentuan itu sudah ada 5 pertanyaan, dan itu sama semua, berarti mungkin dia butuh dilakukan refreshment. Atau mungkin ada pertanyaan-pertanyaan yang memang membutuhkan review kebijakan, ternyata pada pelaksanaan yang tidak bisa, nah itu kita lakukan review kebijakan. Terus di Kepatuhan juga kita sebenarnya melakukan analisa transaksi, ini untuk APU-PPT, itu untuk anti pencucian uang itu bisa dijadikan fraud juga ya sebenarnya, fraud dari pihak eksternal gitu, nah kita juga melakukan analisa transaksi itu pakai sistem setiap bulan.
Mrs Dian Chandra Dewi (28 February 2026)			

Appendix 13. Framework Matrix of Challenges Faced by PT BPR Bank Sleman in Implementing Anti-Fraud Strategies

	RQ 3 Challenges in Implementation	1. Deficiencies	a. Inefficient WBS Mechanism	b. Limited Training Scope
Mr Arif Setiawan (9 December 2025)				
Mr Arif Setiawan (19 February 2026)				
Mr Dwi Handoyo Miharjo (9 December 2025)				
Mr Dwi Handoyo Miharjo (2 February 2026)				
Mrs Rizky Chitra (10 December 2025)				Untuk saat ini belum ada, yang diwajibkan saat ini adalah pelatihan strategi anti fraud bagi seluruh pegawai. Tim Anti Fraud secara berkala melakukan sosialisasi terkait SAF. Untuk pelatihan digital fraud saat ini belum pernah dilaksanakan.
Mrs Rizky Chitra (22 December 2025)				Untuk saat ini belum ada pelatihan khusus. Hanya saja untuk Tim Anti Fraud lebih sering mengikuti pelatihan baik secara offline atau online terkait SAF dibanding dengan pegawai di unit kerja lainnya. Untuk saat ini belum ada. Tapi kedepannya untuk bagian IT ataupun bagian terkait akan dilakukan sertifikasi berkala terkait keamanan sistem dan hal lain yang berkaitan. R : Apakah diadakan pelatihan atau pembekalan keterampilan lainnya kepada pegawai untuk menunjang kinerjanya dalam melakukan surprise audit? Jika ada, bentuk pelatihan atau pembekalan keterampilan dan pengetahuan yang seperti apa dan bagaimana proses, outcome dan kekurangannya? I : Saat ini belum ada dan rencananya akan diberikan pelatihan di tahun 2026.
Mrs Rizky Chitra (19 February 2026)				

	c. Lack of Digital Competency	d. Low Understanding of Provisions	e. Poor Training Design
Mr Arif Setiawan (9 December 2025)			
Mr Arif Setiawan (19 February 2026)			
Mr Dwi Handoyo Miharjo (9 December 2025)			
Mr Dwi Handoyo Miharjo (2 February 2026)			
Mrs Rizky Chitra (10 December 2025)	Ada gap generasi terhadap proses digitalisasi. Seperti pada umumnya, untuk pegawai dengan usia di atas 45 tahun lebih sulit beradaptasi dengan proses digitalisasi dibanding pegawai dengan usia produktif.		
Mrs Rizky Chitra (22 December 2025)		Pemahaman regulasi dan kebijakan, masih banyak pegawai yang belum memahami terkait regulasi dan kebijakan.	Belum ada indikator kinerja sebelum dan sesudah pelatihan. narasumber yang kurang mumpuni di bidangnya.
Mrs Rizky Chitra (19 February 2026)			

	2. Implementation Barriers	a. Low Early Risk Awareness	b. Hesitant to Use WBS
Mr Arif Setiawan (9 December 2025)			
Mr Arif Setiawan (19 February 2026)			
Mr Dwi Handoyo Miharjo (9 December 2025)		Oke, jadi kalau untuk di Management Risk, kendalanya itu sebenarnya ini ya, jadi bagaimana upaya untuk membuat kesadaran risiko sejak dini di seluruh karyawan. Nah itu akan menjadi pr juga, karena seluruh karyawan ini kan tujuannya berbeda-beda. Contoh misalnya Marketing, tujuannya target. Contoh Umum, tujuannya bagaimana operasional kantor berjalan dengan baik. Nah, ketika kita menetapkan risiko di seluruh unit kerja, itu mungkin mereka memahami dan melaksanakan. Tetapi untuk secara keberlangsungan, untuk oh ini berisiko tinggi, ini berisiko itu, mungkin kita masih butuh upaya untuk mengoptimalkan ya. Jadi, belum seratus persen saya sampaikan terkait dengan tingkat kesadaran risiko. Nah itu yang menjadi pr sih bagi kita.	
Mr Dwi Handoyo Miharjo (2 February 2026)			
Mrs Rizky Chitra (10 December 2025)		Untuk saat ini belum ada, yang diwajibkan saat ini adalah pelatihan strategi anti fraud bagi seluruh pegawai. Tim Anti Fraud secara berkala melakukan sosialisasi terkait SAF.	
Mrs Rizky Chitra (22 December 2025)		Awareness pegawai. Kesadaran akan risiko fraud serta kurangnya keberanian pegawai untuk melaporkan kejadian yang dicurigai sebagai tindakan fraud. Pemahaman regulasi dan kebijakan, masih banyak pegawai yang belum memahami terkait regulasi dan kebijakan. I : Belum ada indikator kinerja sebelum dan sesudah pelatihan. I : Kurangnya konsentrasi peserta pada saat pelatihan	Awareness pegawai. Kesadaran akan risiko fraud serta kurangnya keberanian pegawai untuk melaporkan kejadian yang dicurigai sebagai tindakan fraud. Bank Sleman memiliki pedoman terkait WBS dan sudah di-share di portal ketentuan internal sehingga setiap pegawai dapat mengakses secara bebas. Pada saat sosialisasi di setiap unit kerja, Tim Anti Fraud juga menjelaskan terkait WBS. Kekurangannya pegawai masih kurang aware terkait WBS dan masih takut untuk mengungkap kecurangan ataupun fraud di unit kerjanya.
Mrs Rizky Chitra (19 February 2026)			

	c. Perceived Lack of Evidence to Report	d. Human Error
Mr Arif Setiawan (9 December 2025)		
Mr Arif Setiawan (19 February 2026)		
Mr Dwi Handoyo Miharjo (9 December 2025)		
Mr Dwi Handoyo Miharjo (2 February 2026)		
Mrs Rizky Chitra (10 December 2025)		Ada gap generasi terhadap proses digitalisasi. Seperti pada umumnya, untuk pegawai dengan usia di atas 45 tahun lebih sulit beradaptasi dengan proses digitalisasi dibanding pegawai dengan usia produktif.
Mrs Rizky Chitra (22 December 2025)		Pemahaman regulasi dan kebijakan, masih banyak pegawai yang belum memahami terkait regulasi dan kebijakan. I : Belum ada indikator kinerja sebelum dan sesudah pelatihan. R : Faktor apa yang menyebabkan pelatihan tidak efektif? I : Kurangnya konsentrasi peserta pada saat pelatihan, narasumber yang kurang mumpuni di bidangnya. Untuk tim SAF sebaiknya diikutkan sertifikasi namun kendala waktu dan terbatasnya lembaga yang memiliki izin terkait sertifikasi tersebut.
Mrs Rizky Chitra (19 February 2026)		

	RQ 3 Challenges in Implementation	1. Deficiencies	a. Inefficient WBS Mechanism	b. Limited Training Scope
Mrs Dian Chandra Dewi (9 December 2025)			Tapi dari kendala yang di web itu, itu memang juga belum sempurna ya, karena harusnya kan dia bukan satu form yang harus di-download, kemudian di-scan, habis itu di-upload, itu kan agak menyulitkan sebenarnya untuk whistleblower ya. Nah, itu kendalanya juga di situ, jadi kita sebenarnya mau merubah itu jadi langsung inputan, langsung masuk ke whistleblowing officer. Tapi memang untuk pengembangan itu harus membutuhkan waktu, jadi untuk sementara kita menggunakan itu. Cuma ya itu tadi kendalanya harus di-print dulu, harus diisi, harus di-upload, kayak gitu.	
Mrs Dian Chandra Dewi (28 February 2026)				
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman				

	c. Lack of Digital Competency	d. Low Understanding of Provisions	e. Poor Training Design
Mrs Dian Chandra Dewi (9 December 2025)			
Mrs Dian Chandra Dewi (28 February 2026)			
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman			

	2. Implementation Barriers	a. Low Early Risk Awareness	b. Hesitant to Use WBS
Mrs Dian Chandra Dewi (9 December 2025)			Terus kendalanya itu juga ada kalau untuk, kadang kan orang takut juga ya untuk melaporkan gitu ya, mungkin kalau bawahan untuk melaporkan atasannya kayak gitu kan, walaupun sebenarnya aman, kita sudah mensosialisasikan juga, tapi kadang memang masih ada takut di-blacklist, kadang-kadang itu jadi juga kendala whistleblowing, walaupun sebenarnya sudah tanpa nama seperti itu, cuman ya itu juga masih menjadi kendala, jadi kayak angkanya whistleblowing itu masih rendah.
Mrs Dian Chandra Dewi (28 February 2026)			
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman			

	c. Perceived Lack of Evidence to Report	d. Human Error
Mrs Dian Chandra Dewi (9 December 2025)	Kendalanya itu adalah ketika ada pelaporannya, tapi tidak terdapat buktinya. Jadi SDM harus mencari dulu, ini apakah memang betul atau tidak. Nah, kemudian kalau memang tidak ada buktinya, kemudian itu cuma kayak gosip atau apa, itu kan tidak bisa ditindaklanjuti.	Sebenarnya sudah banyak yang kita lakukan, cuma kan memang tidak sempurna gitu ya. Karena memang dari sistem pun, kalau bukan dari individunya sendiri, yang memang membatasi untuk melakukan fraud itu, itu akan sulit gitu. Karena kayak sistem tadi lakukan sistem ini, itu tetap bisa, lama-lama dia akan tahu, oh nanti ada konfirmasi, lama-lama dia akan pasti tahu celahnya ya. Jadi kalau sistem pun sebenarnya masih ada ruang gitu, jadi harus kita kemampuan perbaikan setiap tahun. Dan kalau ada terjadi fraud tadi, kita bisa lihat, oh kenapa ini bisa terjadi fraud, kekurangan kita apa. Mungkin memang sosialisasi ya, misalkan fraud yang memang terjadi dekat gitu, jadi memang di karyawan sendiri tumbuh, karyawan tidak ada niat untuk melakukan fraud, dan dia jadi sadar bahwa, oh nanti kalau aku fraud, aku bisa dipenjara, aku bisa di-blacklist. Memang sistem baik ya, memang bisa menghalau, tapi memang dari orangnya sendiri, jadi kita harus meningkatkan kesadaran fraud, kita juga ada setiap bulan itu ada pengajian, mungkin biar kalau mereka, kalau kaya gitu tuh dosa, dari sisi keyakinannya.
Mrs Dian Chandra Dewi (28 February 2026)		
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman		

Appendix 14. Framework Matrix of Recommended Improvements in Enhancing the Implementation of Anti-Fraud Strategy at PT BPR Bank Sleman

	RQ 4 Recommended Improvements	1. Real Case Discussion	2. Wider and Detailed Training
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman			
Mr Arif Setiawan (9 December 2025)		Ya, mungkin untuk pelatihan, kalau bisa untuk peningkatan kompetensi kan, tidak harus yang massal ya. Paling nggak kan refreshment atau group discussion yang bisa rutin, paling nggak berapa orang, jadi mungkin bisa lebih mendalam, lebih tersampaikan seperti itu.	
Mr Arif Setiawan (19 February 2026)			
Mrs Rizky Chitra (10 December 2025)			
Mrs Rizky Chitra (22 December 2025)			Untuk saat ini belum ada pelatihan khusus. Hanya saja untuk Tim Anti Fraud lebih sering mengikuti pelatihan baik secara offline atau online terkait SAF dibanding dengan pegawai di unit kerja lainnya.
Mrs Rizky Chitra (19 February 2026)			
Mr Dwi Handoyo Miharjo (9 December 2025)		Oke, jadi kalau untuk di Management Risk, kendalanya itu sebenarnya ini ya, jadi bagaimana upaya untuk membuat kesadaran risiko sejak dini di seluruh karyawan. Nah itu akan menjadi pr juga, karena seluruh karyawan ini kan tujuannya berbeda-beda. Contoh misalnya Marketing, tujuannya target. Contoh Umum, tujuannya bagaimana operasional kantor berjalan dengan baik. Nah, ketika kita menetapkan risiko di seluruh unit kerja, itu mungkin mereka memahami dan melaksanakan. Tetapi untuk secara keberlangsungan, untuk oh ini berisiko tinggi, ini berisiko itu, mungkin kita masih butuh upaya untuk mengoptimalkan ya. Jadi, belum seratus persen saya sampaikan terkait dengan tingkat kesadaran risiko. Nah itu yang menjadi pr sih bagi kita.	Rekomendasi untuk di Management Risk tentu kita ingin mendapatkan pelatihan-pelatihan yang lebih detail lagi, lebih dalam lagi, Nah, di sisi lain memang fraud itu bukan cuman dari, yang bukan cuman diketahui oleh unit kami, unit Management Risk. Tapi harapannya kami juga ingin pelatihan lebih detail juga itu disampaikan ke seluruh unit kerja.
Mr Dwi Handoyo Miharjo (2 February 2026)			

	3. Digital System Enhancement	4. Ethics Reinforcement	5. Competence Certification Issuance
Guideline for Anti-Fraud Strategy Implementation at PT BPR Bank Sleman			
Mr Arif Setiawan (9 December 2025)			
Mr Arif Setiawan (19 February 2026)			
Mrs Rizky Chitra (10 December 2025)			
Mrs Rizky Chitra (22 December 2025)		Kurangnya konsentrasi peserta pada saat pelatihan,	Untuk tim SAF sebaiknya diikutkan sertifikasi namun kendala waktu dan terbatasnya lembaga yang memiliki izin terkait sertifikasi tersebut.
Mrs Rizky Chitra (19 February 2026)			
Mr Dwi Handoyo Miharjo (9 December 2025)	bahkan mungkin kita membutuhkan aplikasi-aplikasi yang tadi kan mbak sudah menyinggung digitalisasi di awal. Mungkin aplikasi secara digital yang lebih efektif lagi. Jadi kita bisa mengantisipasi hal-hal potensi terjadinya kecurangan itu.		
Mr Dwi Handoyo Miharjo (2 February 2026)			

	RQ 4 Recommended Improvements	1. Real Case Discussion	2. Wider and Detailed Training
Mrs Dian Chandra Dewi (9 December 2025)		Kalau pelatihan kan memang, kita terus ya, kita sosialisasikan, kemudian kita juga kasih contoh-contoh, mungkin sebenarnya yang paling, apa ya, mengena itu ya kayak contoh-contoh itu, ya. Atau mungkin kalau ada terjadi fraud internal di Bank Sleman gitu kita bisa sampaikan dampaknya seperti apa agar lebih mengena gitu. Karena real terjadi dan kita bisa lihat sendiri sekarang orangnya seperti apa keadaannya. Atau kita juga bisa sharing dengan bank-bank lain, kan itu banyak ya yang ada di internet, kita bisa ambil itu.	
Mrs Dian Chandra Dewi (28 February 2026)			

	3. Digital System Enhancement	4. Ethics Reinforcement	5. Competence Certification Issuance
Mrs Dian Chandra Dewi (9 December 2025)	Tapi dari kendala yang di web itu, itu memang juga belum sempurna ya, karena harusnya kan dia bukan satu form yang harus di-download, kemudian di-scan, habis itu di-upload, itu kan agak menyulitkan sebenarnya untuk whistleblower ya. Nah, itu kendalanya juga di situ, jadi kita sebenarnya mau merubah itu jadi langsung inputan, langsung masuk ke whistleblowing officer. Tapi memang untuk pengembangan itu harus membutuhkan waktu, jadi untuk sementara kita menggunakan itu. Cuma ya itu tadi kendalanya harus di-print dulu, harus diisi, harus di-upload, kayak gitu. Sebenarnya sudah banyak yang kita lakukan, cuma kan memang tidak sempurna gitu ya. Karena memang dari sistem pun, kalau bukan dari individunya sendiri, yang memang membatasi untuk melakukan fraud itu, itu akan sulit gitu. Karena kayak sistem tadi lakukan sistem ini, itu tetap bisa, lama-lama dia akan tahu, oh nanti ada konfirmasi, lama-lama dia akan pasti tahu celahnya ya. Jadi kalau sistem pun sebenarnya masih ada ruang gitu, jadi harus kita kemampuan perbaikan setiap tahun Memang sistem baik ya, memang bisa menghalau, tapi memang dari orangnya sendiri, jadi kita harus meningkatkan kesadaran fraud, kita juga ada setiap bulan itu ada pengajian, mungkin biar kalau mereka, kalau kaya gitu tuh dosa, dari sisi keyakinannya.	Sebenarnya sudah banyak yang kita lakukan, cuma kan memang tidak sempurna gitu ya. Karena memang dari sistem pun, kalau bukan dari individunya sendiri, yang memang membatasi untuk melakukan fraud itu, itu akan sulit gitu. Memang sistem baik ya, memang bisa menghalau, tapi memang dari orangnya sendiri, jadi kita harus meningkatkan kesadaran fraud, kita juga ada setiap bulan itu ada pengajian, mungkin biar kalau mereka, kalau kaya gitu tuh dosa, dari sisi keyakinannya.	
Mrs Dian Chandra Dewi (28 February 2026)			