

ANALYSIS OF AUDIT CHALLENGES IN FRAUD PREVENTION EFFORTS IN THE BANKING INDUSTRY AT BSI KCP SUDIRMAN ATAS, PEKANBARU CITY

Adinda Dyscha¹

Islamic Banking Study Program, Faculty of Sharia and Law
State Islamic University of Sultan Syarif Kasim Riau, Pekanbaru, Indonesia

Email: adindadyscha12345@gmail.com

Abstract

This study aims to analyze the various challenges faced by auditors in detecting and preventing fraud in the Islamic banking industry, specifically at Bank Syariah Indonesia (BSI) KCP Sudirman Atas, Pekanbaru City. As one of the Islamic economic centers in Sumatra, Pekanbaru particularly the Sudirman Atas area faces unique risk dynamics alongside increasing banking digitalization. The research method used is descriptive qualitative with a literature review and case analysis approach. The results indicate that the main audit challenges include the complexity of sharia based transactions, limited auditor competency in information technology, and the risk of human error that creates loopholes for fraud. This study also relates these findings to recent disruptions in Islamic banking services suspected to be linked to cyberattacks and weaknesses in internal control systems. In conclusion, strengthening technology based auditing (continuous auditing), improving auditor competencies, and enhancing human resource integrity are key strategies for fraud mitigation in the future, particularly at BSI KCP Sudirman Atas Pekanbaru.

Keywords: *Islamic Internal Audit, Islamic Banking Fraud, Internal Control*

A. INTRODUCTION

The Islamic banking industry in Indonesia has experienced very rapid growth over the past decade. As the country with the largest Muslim

population in the world, Indonesia possesses significant market potential for the development of sharia-based financial instruments. Pekanbaru, as the capital city of Riau, has become one of the driving forces of the Islamic economy in the Sumatra region. This development is supported by local government policies that encourage the strengthening of the Islamic financial sector, as well as increasing public literacy regarding Islamic banking products (OJK, 2022).

In the local context, the presence of Bank Syariah Indonesia (BSI) KCP Sudirman Atas Pekanbaru serves as an important representation in supporting such growth. As one of the sub-branch offices located in the strategic Sudirman Atas area, BSI plays a significant role in fund collection activities and the distribution of sharia-based financing. The high volume of transactions conducted within this unit directly increases operational complexity as well as the potential risks faced, including the risk of fraud.

Nevertheless, the growth of assets and market expansion in Islamic banking cannot be separated from the threat of financial crimes. According to the report of the Association of Certified Fraud Examiners (ACFE) Indonesia, the banking sector remains the sector most vulnerable to fraudulent activities compared to other sectors (ACFE Indonesia, 2020). In the context of Islamic banking, fraud not only results in financial losses but also affects morality and trust, which are the primary foundations of the Islamic financial system. Therefore, any indication of fraud within institutions such as BSI KCP Sudirman Atas Pekanbaru has the potential to significantly reduce public trust.

Audit challenges in fraud prevention efforts within Islamic banking also tend to be more complex than those in conventional banking. Auditors are not only required to ensure compliance with Financial Accounting Standards (SAK), but must also guarantee conformity with sharia principles (sharia compliance). This dual supervisory function often creates coordination gaps that may be exploited by irresponsible parties to manipulate transactions, particularly those based on contractual agreements (akad) (Haryani &

Suwandi, 2021). In practice, at branch-level operations such as BSI KCP Sudirman Atas Pekanbaru, the limited availability of auditors possessing dual competencies presents a particular challenge in maintaining the quality of supervision.

In addition, the dynamics of the Islamic banking industry in Pekanbaru are also confronted with the acceleration of service digitalization. Digital transformation that is not accompanied by strengthened cybersecurity systems and technology-based audit mechanisms will increase the risk of cyber fraud. Recent phenomena, such as viral cases involving the loss of customers' account balances and disruptions in national Islamic banking service systems, indicate that internal control systems and audit functions are currently under significant pressure. This condition also affects regional operational units, including BSI KCP Sudirman Atas Pekanbaru, both directly and indirectly in terms of customer trust.

The main issue raised in this study is how auditors in the Islamic banking industry, particularly at BSI KCP Sudirman Atas Pekanbaru, are able to navigate the challenges between operational efficiency demands and the effectiveness of fraud detection. The limited number of human resources possessing multidisciplinary competencies in accounting, sharia, and information technology is one of the factors that increases the risk of undetected fraud. Ultimately, this risk may have serious implications for institutional reputation and the stability of the Islamic banking industry as a whole (Mulyadi, 2020).

Therefore, this research is important in order to provide a more comprehensive mapping of audit challenges and to formulate fraud prevention strategies that are more adaptive to technological developments and contemporary risk dynamics, particularly within the operational context of BSI KCP Sudirman Atas Pekanbaru.

B. METHOD

This study employs a descriptive qualitative method with a case study and literature analysis approach. This approach was chosen to obtain an in-depth

understanding of the phenomenon of audit challenges in fraud prevention efforts, particularly at Bank Syariah Indonesia KCP Sudirman Atas, Pekanbaru, as the research context.

The data sources in this study consist of secondary data obtained through the following data collection techniques:

1. Literature Review

The research was conducted by examining various scholarly sources such as national and international journals, reference books, banking annual reports, and statistical data published by the Financial Services Authority (OJK) during the 2019–2024 period. This literature review aims to establish a strong theoretical foundation related to Islamic internal auditing, banking fraud, and internal control syst.

2. Content Analysis

The researcher analyzed various news articles, official reports, and media publications related to fraud cases and system disruptions in Islamic banking in Indonesia. This analysis focused on identifying patterns of incidents, causal factors, and the resulting impacts, particularly those relevant to branch-level operations such as Bank Syariah Indonesia KCP Sudirman Atas Pekanbaru.

3. Secondary Observation

Observations were conducted indirectly through monitoring developments in the Islamic banking industry in Pekanbaru City, especially in the Sudirman Atas area, based on regional publication reports, statistical data, and trends in the growth of Islamic banking services.

The data analysis technique used in this study refers to the interactive analysis model developed by Matthew B. Miles and A. Michael Huberman, which consists of three main stages: data reduction, data presentation, and conclusion drawing. The data reduction process was carried out by filtering information relevant to the research focus, which was then systematically

presented in descriptive narrative form and concluded through interpretative analysis.

In this study, the analysis focused on several key variables, namely audit challenges, the effectiveness of internal control systems, and the factors driving the occurrence of fraud. These variables were analyzed using the Fraud Diamond Theory approach, which includes four main elements: pressure, opportunity, rationalization, and capability (Fahri & Rahayu, 2023). This approach was employed to provide a more comprehensive understanding of the factors causing fraud within the operational context of Bank Syariah Indonesia KCP Sudirman Atas, Pekanbaru City.

C. RESULTS AND DISCUSSION

1. Identification of Audit Challenges in Islamic Banking in Pekanbaru

Based on the analysis results, the audit function in the Islamic banking industry in Pekanbaru faces various complex challenges, including technical, technological, and organizational culture aspects. In this study, the discussion is also associated with the operational context of Islamic banking branches, such as Bank Syariah Indonesia KCP Sudirman Atas Pekanbaru, as a representation of regional operational units. These challenges directly affect the effectiveness of audits in detecting and preventing fraud.

Several major challenges can be described as follows:

- **Complexity of Products and Sharia Compliance**

Islamic banking has unique characteristics that distinguish it from conventional banking, particularly in the use of contracts (*akad*) as the basis of transactions. Auditors are not only responsible for ensuring the accuracy of financial records, but must also verify whether transactions comply with Sharia principles (*sharia compliance*).

- Products such as Murabahah, Mudharabah, Musyarakah, and Ijarah have complex structures and require a deep understanding of *fiqh muamalah*. In practice, fraud opportunities often arise through the manipulation of contract documents, such as profit margin

engineering, concealment of non-performing financing risks, or discrepancies between the contract and its actual implementation in the field.

Sari et al. (2022) stated that weaknesses in the contract verification process are among the vulnerable points for fraud in Islamic banking. In addition, the limited competence of auditors in understanding Sharia aspects may hinder the early detection of irregularities, especially at branch operational levels such as [Bank Syariah Indonesia](#) KCP Sudirman Atas Pekanbaru.

2. Information Technology Competency Gap (IT Audit Gap)

Digital transformation in the banking industry has shifted operational systems toward technology- and data-based processes. Most transactions and records are now conducted electronically (*paperless*), requiring auditors to possess competencies in information technology-based auditing.

However, many internal auditors in regional areas, including Pekanbaru, still predominantly come from conventional accounting backgrounds and do not yet possess adequate competencies in IT auditing. This condition is also relevant as an illustration of the challenges potentially faced by operational units such as Bank Syariah Indonesia KCP Sudirman Atas Pekanbaru.

This situation results in limitations in the use of modern audit techniques such as data analytics, continuous auditing, and computer-assisted audit techniques (CAATs). Consequently, auditors tend to rely on traditional audit methods, which are less effective in detecting digital-based fraud, such as system manipulation, data engineering, or fictitious transactions within information systems. Pratama (2024) emphasized that the lack of mastery of audit technology is one of the main factors hindering audit effectiveness in the digital era.

3. Organizational Culture and Target Pressure

Rapid economic growth in Pekanbaru has intensified competition among banks, including Islamic banks. This condition has encouraged management to set high performance targets, particularly in financing distribution. The

pressure to achieve these targets often leads to the neglect of prudential principles and internal control procedures.

In such situations, employees may be driven to engage in deviant actions, such as manipulating financing data, accelerating approvals without adequate analysis, or concealing risk-related information. Tuanakotta (2019) states that pressure is one of the main elements in the Fraud Triangle that can trigger fraudulent behavior.

In addition, organizational cultures that do not fully emphasize integrity, transparency, and accountability further increase the risk of fraud. Weak whistleblowing systems, lack of protection for whistleblowers, and minimal enforcement of work ethics are factors that worsen this condition, including within the operational environment of Islamic banking branches such as Bank Syariah Indonesia KCP Sudirman Atas Pekanbaru.

Overall, these three challenges indicate that the audit function in Islamic banking in Pekanbaru faces obstacles that are not only technical in nature, but also related to human resources and organizational culture. Therefore, a comprehensive approach is needed to improve audit effectiveness in preventing fraud, including enhancing auditor competencies, utilizing technology, and strengthening an organizational culture based on integrity.

4. Case Analysis: System Disruptions and Fraud Risks

The Indonesian Islamic banking industry was recently shaken by a viral case involving the shutdown of the system of one of the country's largest Islamic banks for several days. Officially, the incident was linked to a ransomware attack; however, from an audit perspective, the incident revealed several fundamental weaknesses that are also relevant as lessons for regional operational units, including Bank Syariah Indonesia KCP Sudirman Atas Pekanbaru:

- **Failure in Disaster Recovery Plan (DRP) Implementation**

The failure in implementing the Disaster Recovery Plan (DRP) indicates that the backup system was not able to function optimally when the main system experienced disruption or total failure. In the context of

information technology risk management, DRP is an integral part of the Business Continuity Plan (BCP), which aims to ensure organizational operational continuity during emergency conditions (Snedaker, 2014). Therefore, internal audit plays a crucial role in evaluating not only the existence of DRP documentation, but also the effectiveness of its actual implementation within the operational environment.

- Internal auditors should conduct periodic testing through simulations or disaster recovery testing to assess the readiness of backup systems in taking over the functions of the main system. This testing includes evaluating important parameters such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO), which determine acceptable limits for recovery time and data loss (Botha & Solms, 2004). Failure to meet RTO and RPO targets may indicate weaknesses in IT infrastructure, inadequate data synchronization, or unprepared technical recovery procedures.

In addition, audits should evaluate the level of integration between the primary data center and the backup data center, including the effectiveness of failover mechanisms, both automatic and manual. If these processes do not function properly, service recovery will experience significant delays and may increase operational and reputational losses. This confirms that DRP failure reflects not only technical weaknesses, but also suboptimal internal audit oversight in ensuring organizational preparedness for critical system disruption risks (Hall, 2016).

- | • Potential | Insider | Threats |
|--|----------------|----------------|
| Cyberattacks do not always originate from external parties; in many cases, they begin with internal factors such as employee negligence, weak credential management, or even intentional collaboration. Insider threats are among the most difficult risks to detect because the perpetrators possess legitimate access to organizational systems. This condition requires internal auditors to develop a more proactive monitoring approach through continuous auditing and the utilization | | |

of analytical technologies to monitor system activities in real time (Prabowo, 2023).

Internal auditors need to evaluate the effectiveness of access controls, including the implementation of the least privilege principle and segregation of duties, in order to minimize the potential for abuse of authority. Furthermore, analysis of log activity and the implementation of user behavior analytics are important instruments for detecting access anomalies, such as unusual login activities, unauthorized access to sensitive data, or system usage patterns that deviate from normal user behavior. Early detection of such indications is essential to prevent the escalation of attacks that may lead to larger system disruptions (Behl & Behl, 2017).

On the other hand, low levels of security awareness among employees also contribute to the increasing risk of insider threats. The lack of cybersecurity training, such as phishing prevention and secure password management, may create vulnerabilities that attackers can exploit through human weaknesses as entry points. Therefore, organizations need to integrate both technical and non-technical approaches in risk mitigation, including educational programs and strengthening information security culture (Whitman & Mattord, 2019).

- **Reputational Impact in Pekanbaru**

a. The system disruption not only affected the bank's internal operations, but also created serious consequences for its reputation and public trust. In Pekanbaru, this incident has the potential to trigger customer panic, marked by massive fund withdrawals (*bank run*). This phenomenon demonstrates that trust is a key factor in maintaining banking system stability (Rose & Hudgins, 2013).

b. Simultaneous large-scale fund withdrawals have the potential to create significant liquidity pressure. This indicates that weaknesses in audit systems and internal controls can directly affect financial stability and institutional reputation (Saunders & Cornett, 2018).

Thus, this incident confirms that information technology risk has evolved into a strategic risk with broad implications for the stability of the financial system. Therefore, internal audit must transform into a more proactive function capable of providing early warnings regarding potential risks (Hall, 2016).

5. The Relationship Between the Fraud Diamond Theory and Islamic Banking

Although financial institutions operate under Islamic principles, fraudulent practices remain a real threat. This indicates that the implementation of sharia principles has not been entirely effective in eliminating the potential for individual misconduct within organizations. Fraud in the Islamic banking industry is fundamentally influenced by the four main elements of the fraud diamond theory, namely pressure, opportunity, rationalization, and capability. These four elements are interconnected and can increase the likelihood of fraudulent activities if they are not managed properly.

In the context of Islamic banking in Pekanbaru, including operational units such as [BSI KCP Sudirman Atas Pekanbaru](#), pressure experienced by employees generally arises from demands to achieve performance targets, particularly in financing distribution and fund collection. Such pressure often encourages individuals to seek shortcuts in order to meet targets within a specified timeframe. In addition, personal financial needs also become a contributing factor that cannot be ignored.

Furthermore, opportunity arises due to weak internal control systems and ineffective supervision. For example, inadequate segregation of duties, weak internal audit systems, and loopholes in standard operating procedures may be exploited by certain individuals. These conditions provide opportunities for individuals to commit fraud without being easily detected, particularly at the branch operational level.

Rationalization is considered a dominant factor in the context of Islamic banking. Fraud perpetrators often justify their actions based on moral reasons or certain objectives that they perceive as beneficial. In the context of

Pekanbaru, rationalization may appear in the form of assumptions that such actions are intended to help customers experiencing financial difficulties or to achieve the bank's welfare objectives. However, these actions still violate prudential principles and applicable sharia regulations. This reflects a misunderstanding of the concept of *maslahat* (public benefit) from an Islamic perspective (Zainal et al., 2021).

In addition, capability also plays an important role in the occurrence of fraud. Individuals who possess extensive knowledge of banking operational systems and have access to sensitive information are generally more capable of committing and concealing fraudulent acts. This capability is usually supported by long work experience and strategic positions within the organization.

Based on the analysis above, it can be concluded that although Islamic banking is founded on the values of honesty, trustworthiness, and justice, human factors remain a crucial element in the potential occurrence of fraud. Therefore, comprehensive preventive measures are required, such as strengthening internal control systems, improving the quality of sharia audits, and instilling ethical values and integrity based on Islamic principles among all human resources within the organization.

6. Fraud Prevention Efforts in the Banking Industry

Fraud prevention efforts in the banking industry in Pekanbaru require a comprehensive and integrated approach that includes audit practices, internal control systems, and human resource management. In this study, these strategies are also relevant to the operational context of branch offices such as [BSI KCP Sudirman Atas Pekanbaru](#) as a representation of Islamic banking at the regional level.

Based on the findings of this study, several strategies can be implemented to minimize the risk of fraud.

First, improving auditor competence is an important step in strengthening the supervisory function. Auditors need to be equipped with relevant training, particularly in the field of information technology, in order to detect potential

digital-based fraud. This is in line with the study conducted by Sari and Putra (2022), which states that digital-based auditor competence has a significant effect on the effectiveness of audits in detecting fraud.

Second, strengthening the internal control system must be carried out comprehensively. Organizations need to ensure clear segregation of duties, effective monitoring systems, and structured audit procedures. According to Wibowo (2021), strong internal control systems have been proven to reduce the level of fraud within banking organizations.

Third, maintaining auditor independence is a crucial factor in ensuring the objectivity of audit results. Auditors must be free from pressure or intervention from management in order to disclose findings transparently. Rahmawati (2023) states that auditor independence significantly influences audit quality and fraud prevention.

Fourth, the utilization of audit technology, such as data analytics and digital-based audit systems, can assist auditors in detecting transaction anomalies more quickly and accurately. This is supported by Pratama (2024), who emphasizes the importance of technology utilization in modern auditing processes.

Fifth, establishing an anti-fraud organizational culture is also a strategic step. This can be achieved through socialization programs, ethics training, and the implementation of a whistleblowing system. Hidayat (2022) states that a strong organizational culture and effective reporting systems can significantly reduce the occurrence of fraud.

Therefore, fraud prevention efforts do not solely depend on the audit function, but also require synergy among improving auditor competence, strengthening internal control systems, utilizing technology, and building an organizational culture based on integrity.

D. Conclusion

Based on the results of the analysis and discussion, it can be concluded that the risk of fraud in the Islamic banking industry in Pekanbaru is a complex issue influenced by various interrelated factors, including audit technicalities,

technological developments, and organizational culture. In this study, these dynamics are also associated with the operational context of Islamic banking branches, such as [BSI KCP Sudirman Atas Pekanbaru](#), as a representation of regional-level operational units. As one of the centers of Islamic economic growth in Sumatra, Pekanbaru faces increasingly significant risk dynamics alongside the expansion of banking services and digitalization.

The findings of this study indicate three major challenges faced by auditors in detecting and preventing fraud, namely the complexity of sharia contract-based products, the gap in auditors' competence in information technology (IT audit gap), and organizational pressure influenced by performance targets and work culture. The complexity of sharia transactions requires auditors to possess dual competencies in accounting and sharia compliance. A lack of such competencies may create opportunities for manipulation. On the other hand, limited mastery of audit technology reduces auditors' effectiveness in detecting increasingly sophisticated forms of digital fraud. Furthermore, performance pressure and weak organizational integrity culture also increase the likelihood of fraudulent activities, particularly at the branch operational level.

The analysis of cases involving disruptions in the national Islamic banking system also demonstrates that weaknesses in internal control systems, especially in the areas of information technology and risk management, can have widespread impacts and reduce public trust. This confirms that fraud in the digital era does not only originate from individual factors, but also from failures in systems and organizational governance.

Furthermore, this study confirms the relevance of the Fraud Diamond Theory in the context of Islamic banking, where the factors of pressure, opportunity, rationalization, and capability remain the primary determinants of fraud, even within institutions founded upon sharia principles.

Therefore, future fraud prevention efforts must be implemented comprehensively and continuously. Strengthening technology-based auditing practices, such as continuous auditing, improving auditors' competencies

particularly in information technology and sharia, and reinforcing internal control systems are strategic measures that should be prioritized. In addition, establishing an organizational culture that upholds integrity, transparency, and accountability is essential in creating an Islamic banking system that is resilient against fraud.

As a recommendation, future studies are expected to empirically examine the effectiveness of audit technology implementation in regional Islamic banking institutions, including at the branch level, and to explore more deeply the integration model between sharia audit and information technology audit. Moreover, quantitative studies using primary data are also necessary to objectively measure the influence of the variables identified in this research.

References

- [Association of Certified Fraud Examiners \(ACFE\)](#) (2022). *Report to the Nations*. Association of Certified Fraud Examiners (ACFE) Indonesia. (2020). *Indonesia Fraud Survey 2019*. Jakarta: ACFE Indonesia.
- [Bank Syariah Indonesia](#) (2024). *Annual Report 2023*.
- Botha, J., & von Solms, R. (2004). *A cyclic approach to business continuity planning*. *Information Management & Computer Security*, 12(4), 328–337.
- Fahri, M., & Rahayu, S. (2023). *Analysis of Fraud Diamond Theory in Detecting Financial Fraud*. *Journal of Accounting and Finance*, 11(2), 120–135.
- Hall, J. A. (2016). *Information Technology Auditing* (4th ed.). Cengage Learning.
- Haryani, S., & Suwandi, A. (2021). *Dualism of Supervision in Islamic Banking and Its Implications for Fraud*. *Journal of Islamic Economics*, 9(1), 45–58.
- Hidayat, M. (2022). *Organizational Culture and Fraud Prevention through a Whistleblowing System*. *Journal of Management and Business*, 12(3), 210–225.
- International Auditing and Assurance Standards Board (2021). *International Standards on Auditing*.

- Ministry of Finance of the Republic of Indonesia (2023). *Development of the Islamic Economy in Indonesia*.
- Mulyadi. (2020). *Accounting Systems* (Revised Edition). Jakarta: Salemba Empat.
- Otoritas Jasa Keuangan (2022). *Report on the Development of Islamic Banking in Indonesia 2022*. Jakarta: OJK.
- Otoritas Jasa Keuangan (2024). *Islamic Banking Statistics of Indonesia*.
- Prabowo, A. (2023). *Risk Analysis of Insider Threats in Information System Security*. *Indonesian Cybersecurity Journal*, 5(2), 45–56.
- Prabowo, R. (2023). *Analysis of Insider Threat Risks in Cyber Attacks on Banking*. *Journal of Information Security*, 7(1), 55–70.
- Pratama, R. (2024). *Utilization of Data Analytics in Auditing to Detect Fraud*. *Journal of Accounting Information Systems*, 6(2), 88–102.
- Rahmawati, D. (2023). *Auditor Independence and Its Influence on Audit Quality*. *Indonesian Journal of Auditing*, 8(1), 33–47.
- Sari, N., & Putra, A. (2022). *The Influence of Auditor Competence on Fraud Detection in the Digital Era*. *Journal of Accounting and Auditing*, 10(2), 75–90.
- Snedaker, S. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals* (2nd ed.). Syngress.
- Tuanakotta, T. M. (2019). *Forensic Accounting and Investigative Auditing* (2nd ed.). Jakarta: Salemba Empat.
- Wibowo, T. (2021). *The Effectiveness of Internal Control in Fraud Prevention in Banking*. *Journal of Finance and Banking*, 15(1), 60–74.
- Zainal, A., et al. (2021). *Implementation of the Fraud Diamond in Detecting Fraud in Islamic Banking*. *Journal of Islamic Economics and Business*, 8(2), 140–155.