Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 9, Issue 1 (January-June) 2024
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

Analysis of Fraud Patterns in Islamic Banking Transactions: Strategies and Implementation of Prevention

✉Khairul Katsirin
IAI Sultan Muhammad Syafiuddin Sambas, Islamic Economics and Business, Sambas, Kalimantan Barat, Indonesia

ARTICLE INFORMATION
Article History:
Received October 2, 2023
Revised January 2, 2024
Accepted June 4, 2024

DOI:
10.21532/apfjournal.v9i1.321

ABSTRACT
The research aims to analyze patterns of fraud in Sharia banking transactions and identify effective prevention strategies. The method used is a qualitative approach with case study data collection. The research findings reveal various common patterns of fraud, such as identity theft, document forgery, transaction manipulation, and misappropriation of funds. Factors such as weaknesses in the transaction system, weak security policies, and lack of employee training influence the occurrence of fraud. Prevention strategies that can be implemented include early detection systems, strict security policies, employee training, and cooperation with authorities. It is hoped that the research findings can assist Sharia banks in enhancing transaction security, protecting customers, and minimizing fraud risks.

Keyword: Fraud, Islamic Banking Transactions, Fraud Patterns, Prevention Strategies, Transaction Security

1. INTRODUCTION

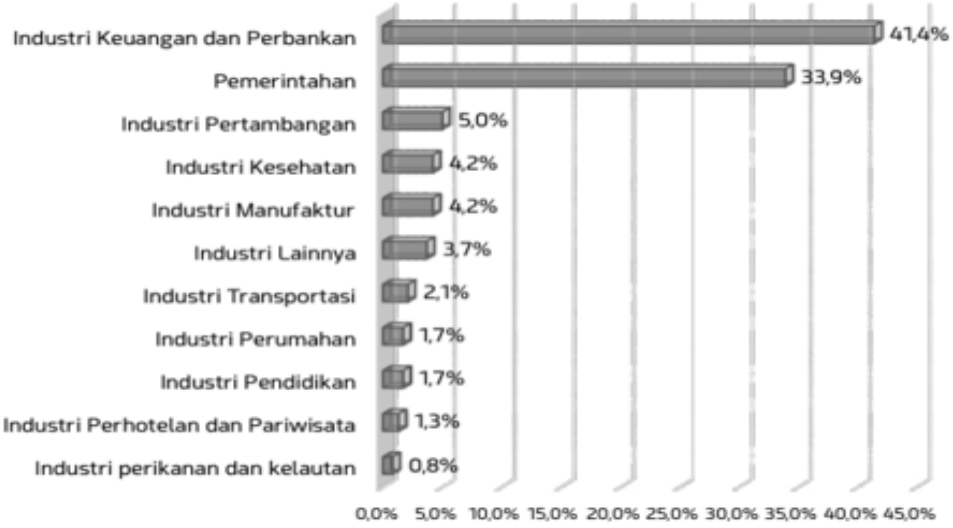
Islamic banks are financial institutions operating based on Sharia principles, which include prohibitions against usury (interest) and transactions involving uncertainty or speculation. With the growth and development of the Islamic banking industry, the challenges in maintaining the integrity of the Islamic banking system have also become increasingly complex. One of the challenges faced by Islamic banks is fraud in banking transactions.

According to survey data from the *Association of Certified Fraud Examiners* (ACFE), the financial and banking industry in Indonesia experienced significantly damaging fraud incidents in 2019, ranking first at 41.4%. This data indicates that fraud cases in the financial and banking sector are a serious issue that demands attention. Shariah-compliant banks, as part of the financial sector, are not exempt from the risk of fraud, which can jeopardize the integrity and public trust in the Islamic banking system.

How to Cite:
Katsirin K., (2023). Analysis of Fraud Patterns in Islamic Banking Transactions: Strategies and Implementation of Prevention. *Asia Pacific Fraud Journal, 9*(1), 81-89. http://doi.org/10.21532/apfjournal.v9i1.321.

✉Corresponding author :
Email: khairulkatsirin@gmail.com

Figure 1. **Results of Fraud Survey in Indonesia 2019**



Source: ACFE Indonesia Chapter, 2020

Fraud in Shariah banking transactions can involve activities such as identity theft (Masriadi, 2019), document forgery (Nasution, 2022), embezzlement of funds (Newswire, 2021), or unauthorized use of personal information (Ayyubi, 2021). Such fraud can lead to significant financial losses for Islamic banks and their customers, as well as damage the overall reputation of the Islamic banking industry.

To address these challenges, it is crucial to conduct a comprehensive analysis of the fraud patterns occurring in Shariah banking transactions. By analyzing common fraud patterns, Islamic banks can identify security gaps that need strengthening and develop more effective prevention strategies.

In addition, effective implementation of prevention measures is also a key factor in addressing fraud in Shariah banking transactions. A sound prevention strategy should encompass steps such as a reliable early detection system, stringent security procedures, appropriate employee training, and a collaborative approach with authorities and regulatory bodies (Rustandy et al., 2020; Sabatina & Wahyudin, 2021; Sudarmanto, 2020; Syahputra & Urumsah, 2019).

Previous research conducted by (Kurniasari et al., 2018) stated that effective strategies for preventing fraud can involve several actions: (1) changing the supervision and control systems, (2) strengthening the organizational culture, (3) formulating anti-fraud policies, (4) implementing a strict rewards and discipline system, (5) employee awareness campaigns, and (6) appointing change agents.

The purpose of conducting this research is to analyze fraud patterns in Shariah banking transactions and identify effective prevention strategies and implementations. Through this research, it is hoped to provide a comprehensive understanding of how fraud occurs in the context of Islamic banking and assist Islamic banks in addressing fraud challenges more effectively. The research findings are expected to make a significant contribution to maintaining the integrity of the Islamic banking system, protecting the interests of customers, and strengthening public trust in Islamic banking.

2. LITERATURE REVIEW AND HYPOTHESIS

Transaction Reliability Theory

Transaction Reliability Theory is a conceptual framework used to analyze and understand the reliability aspects within business transactions. This theory emphasizes the importance of trust, interdependence, and long-term

commitment among parties involved in business transactions. In a complex and dynamic business environment, transaction reliability plays a crucial role in building strong relationships among companies, customers, suppliers, and other stakeholders.

Transaction Reliability Theory was first introduced by Williamson in 1979). and has since become a significant theoretical foundation in economics, management, and related social sciences. According to this theory, transaction reliability can be measured through three main dimensions: information, commitment, and control. The information dimension includes adequate access to and understanding of relevant information in transactions. Transaction Reliability Theory also acknowledges that there are costs associated with building and maintaining transaction reliability. These costs include information search costs, monitoring and contract enforcement costs, as well as costs related to risks and uncertainties in transactions.

The application of Transaction Reliability Theory can offer significant benefits to companies. By establishing transaction reliability, companies can create mutually beneficial relationships, minimize risks, enhance operational efficiency, and increase customer satisfaction. Transaction reliability also contributes to the development and maintenance of a good reputation, which can be a valuable asset in a competitive business environment (Dyer & Singh, 1998; Ghoshal, 1987).

Technology Security Concepts

Technology security is a crucial aspect in today's digital era. Therefore, it is essential for organizations and individuals to understand various technology security concepts to protect sensitive data and information from existing threats. Technology security concepts encompass several aspects, including network security (Al-Kaabi & Belhaouari, 2019), system security (Asllani et al., 2018; Mugarza et al., 2020), application security (Hasan & Suhermanto, 2021), and data security (Siregar, 2020).

Securing technology is a top priority in this digital age. Technology security concepts, such as network security, system security, application security, and data security, must be taken seriously to safeguard organizations and individuals from a variety of security threats.

Fraud Behavior Theory

Fraud Behavior Theory is a theoretical framework that examines the motivations and behaviors behind fraud in the context of Shariah banking transactions. By understanding the factors that drive fraud, we can identify potential fraud patterns that may occur. Several factors often associated with fraudulent behavior include financial pressure, opportunity, and rationalization (Isgiyata et al., 2018; Vona, 2012).

Financial pressure is often a primary driver of fraudulent actions. Individuals facing significant financial pressures, such as mounting debts or urgent needs, may be tempted to commit fraud as a means to meet their financial requirements (Hormati et al., 2019). In the context of Shariah banking transactions, understanding these financial pressure factors can help identify fraud risks related to the financial conditions of individuals or businesses.

Additionally, opportunity is a factor that influences fraudulent behavior. When someone has access and the opportunity to commit fraud without being detected, their motivation to do so may increase (Faradiza, 2018). In Shariah banking transactions, weaknesses in supervision and control systems can create opportunities for individuals or groups to engage in fraud. Therefore, understanding these opportunity factors is crucial in developing effective prevention strategies.

Rationalization is also a factor that plays a role in fraudulent behavior. Individuals tend to rationalize their actions to justify them, even when they are aware that it is unethical behavior (Kismawadi et al., 2020). Rationalization can include reasons such as feeling "entitled" to what they steal or convincing themselves that

they are taking something that would "not be missed" by the victim. Understanding these rationalization factors can help recognize justifications used by fraudsters and implement relevant prevention measures.

3. METHODS

This research will adopt a qualitative approach that allows the researcher to gain in-depth understanding of fraud phenomena within Shariah banking transactions. To collect data, a case study will be conducted on Shariah banking transactions involving fraud cases from 2019 to 2023. The collected data will be analyzed using thematic analysis method aimed at identifying and analyzing common fraud patterns that occur in the context of Shariah banking transactions. Through thematic analysis, this research will uncover relevant information on how fraud occurs, tactics used, and several factors that can influence fraud in Shariah banking transactions. Additionally, this research will also identify prevention strategies that can be implemented to mitigate the risk of fraud in Shariah banking transactions. By combining qualitative approach and thematic analysis, it is expected to provide deep insights and significant contributions in addressing fraud issues within Shariah banking transactions.

4. RESULTS AND DISCUSSION

This research has yielded an in-depth understanding of fraud patterns in Shariah banking transactions, the factors influencing fraud, and prevention strategies that can be applied. Here is a summary of the research findings.

Fraud Patterns in Shariah Banking Transactions

In this research, various common fraud patterns were identified in Shariah banking transactions. These fraud patterns include identity theft, document forgery, transaction manipulation, and misappropriation of funds. These findings illustrate the complexity of fraudulent techniques used in the context of Shariah banking.

Identity theft is one of the common fraud patterns in Shariah banking transactions. Fraudsters may use someone else's identity to conduct unauthorized transactions, access customer accounts, or obtain loans in someone else's name. Identity theft often involves the use of personal information obtained through methods such as phishing, system hacking, or identity document theft (Ali et al., 2019; Zulkarnain & Sutabri, 2023).

Document forgery is another frequently occurring fraud pattern in Shariah banking transactions. Fraudsters can forge documents such as identities, powers of attorney, or other documents to gain access to customer accounts, transfer funds, or access confidential information. Document forgery often utilizes advanced technology, including techniques like Photoshop and counterfeit document printing that are difficult to distinguish from genuine documents (Kanika & Singla, 2019).

Transaction manipulation is another common fraud pattern in Shariah banking transactions. Fraudsters may manipulate transaction records, alter the amount or details of transactions, or manipulate the banking system to gain personal benefits. Transaction manipulation typically occurs due to the misuse of authority or knowledge related to the banking system in use (Akinbowale et al., 2023).

Misappropriation of funds is also a frequently occurring fraud pattern in Shariah banking transactions. Fraudsters can use their position or access within banking institutions to divert customer funds or avoid legitimate reporting. Misappropriation of funds often involves the falsification of documentation, abuse of trust, or the diversion of funds through unauthorized channels (Agha, 2007; Datau, 2017).

The findings regarding various fraud patterns in Shariah banking transactions highlight the complexity of fraudulent

techniques used. Shariah banks need to enhance their internal supervision and control systems, employ advanced security technology, and provide training to employees to recognize signs of fraud and take appropriate preventive measures. This is crucial to minimize the risk of fraud, protect customer interests, and maintain the integrity of the Shariah banking sector as a whole.

Factors Influencing Fraud in Shariah Banking Transactions

This research has identified several factors that contribute to fraud in Shariah banking transactions. These factors include weaknesses in transaction systems and technology infrastructure, weak security policies, lack of employee training in recognizing fraud signs, and internal and external factors affecting the operational environment of Shariah banks. These findings emphasize the importance of addressing these factors to prevent fraud.

Weaknesses in transaction systems and technology infrastructure can facilitate fraud in Shariah banking transactions. Vulnerable transaction systems or technical disruptions can allow fraudsters to exploit them. Inadequate technology infrastructure or a lack of security systems can facilitate unauthorized access and data manipulation for fraudulent purposes (Arifah, 2011; Muchlis, 2018).

Weak security policies can provide opportunities for fraud in Shariah banking transactions. When security policies are inadequate or not effectively implemented, the risk of fraud increases. This includes a lack of strong authentication mechanisms, weaknesses in password management, or inadequate security risk management policies (Tsabita et al., 2023).

Lack of employee training in recognizing fraud signs can also influence fraud in Shariah banking transactions. Employees who are not adequately trained to identify fraudulent activities may fail to recognize suspicious fraud patterns. Adequate training in transaction security and fraud detection can enhance fraud prevention (Sudarmanto & Utami, 2021).

Internal and external factors affecting the operational environment of Shariah banks can play a role in fraud. For instance, internal factors such as an organizational culture that is less concerned about security, inadequate supervision and effective control, and ethical violations by employees can impact the risk of fraud (Herlita & Bayunitri, 2021; Reskia & Sofie, 2022). External factors such as regulatory changes, economic instability, or high industry pressure can also create an environment conducive to fraud (Hendrianto et al., 2023).

These findings underscore the importance of addressing the factors influencing fraud in Shariah banking transactions. Efforts are needed to strengthen transaction systems and technology infrastructure, improve security policies, provide adequate training to employees, and foster an organizational culture that values security. Additionally, consideration must be given to external factors that may affect fraud risk, and appropriate measures should be taken to address them.

Fraud Prevention Strategies in Shariah Banking Transactions

This research has generated prevention strategies that can be applied to reduce the risk of fraud in Shariah banking transactions. These prevention strategies include the implementation of advanced early detection systems, the enforcement of strict security policies, employee training to increase awareness of fraud, and close cooperation with authorities. These findings provide practical guidance for Shariah banks in enhancing the security of their banking transactions.

Implementation of advanced early detection systems is one of the effective prevention strategies in reducing fraud risk. Early detection systems use technology and algorithms to analyze transaction data in real-time to identify suspicious fraud patterns. These systems can alert Shariah

banks when unusual activities are detected, allowing for immediate preventive actions to be take (Sumandi, 2017).

Enforcement of strict security policies is also a crucial strategy in fraud prevention. Adequate security policies should include measures such as strong authentication, data encryption, strict access management, and active monitoring of systems and transactions. By implementing strict security policies, Shariah banks can minimize the risk of fraud stemming from cyberattacks and unauthorized access (Munawarah & Yusuf, 2022).

Employee training is another important strategy to increase awareness of fraud. Employees need to be well-informed about common fraud patterns in Shariah banking transactions, as well as techniques for fraud detection and prevention. With adequate training, employees can become more vigilant in spotting signs of fraud, reporting suspicious activities, and taking appropriate preventive measures (Sudarmanto & Utami, 2021)

Close cooperation with authorities is a critical strategy in fraud prevention. Shariah banks need to collaborate with authorities such as law enforcement agencies, banking supervisory authorities, and law enforcement-related agencies. Through this collaboration, Shariah banks can obtain up-to-date information on prevailing fraud patterns and receive support in investigating and prosecuting fraudsters (Mujiatun et al., 2022; Noviatun & Isfandayani, 2020).

These findings offer practical guidance for Shariah banks in enhancing the security of their banking transactions. By implementing advanced early detection systems, enforcing strict security policies, conducting appropriate employee training, and establishing close cooperation with authorities, Shariah banks can reduce the risk of fraud, protect customer interests, and maintain the overall integrity of Shariah banking transactions.

5. CONCLUSION

In this research, various common patterns of fraud in Shariah banking transactions have been revealed, including identity theft, document forgery, transaction manipulation, and fund embezzlement. These findings highlight the complexity of fraud techniques employed by perpetrators within the context of Shariah banking. Factors such as weaknesses in transaction systems, weak security policies, lack of employee training, and internal and external factors also influence the occurrence of fraud.

In addressing the challenge of fraud in Shariah banking transactions, several prevention strategies have been identified. These strategies include the implementation of advanced early detection systems, the enforcement of stringent security policies, effective employee training, and close collaboration with authorities. By implementing these strategies, Shariah banks can enhance transaction security, protect customers, and minimize the risk of fraud.

Here are some recommendations provided by the researcher to improve the security of Shariah banking transactions:

a. Enhance Security Systems: Shariah banks should bolster their security systems by implementing advanced technologies, such as Artificial Intelligence (AI) and big data analytics, to accurately detect fraudulent patterns in real-time.
b. Improve Employee Training: Shariah banks need to provide comprehensive training to their employees to enhance their awareness of fraud indicators and the preventive procedures to follow. This training should be regularly updated to keep pace with evolving fraud techniques.
c. Enhance Collaboration with Authorities: Shariah banks should establish close cooperation with relevant authorities, including banking regu-

lators and law enforcement agencies, to share information, report fraud cases, and take enforcement actions against perpetrators.

d. Increase Customer Awareness: Shariah banks should raise customer awareness about the risks of fraud in Shariah banking transactions and provide education on safe security practices, such as safeguarding personal data confidentiality and not sharing sensitive information with unauthorized parties.
e. Review Policies and Procedures: Shariah banks should periodically review and update their security policies and procedures to align with technological advancements and the latest fraud trends. Additionally, Shariah banks should conduct regular internal audits to ensure compliance with these policies and procedures.

REFERENCES

ACFE Indonesia. (2020). *Survei Fraud Indonesia 2019*. ACFE Indonesia. https://acfe-indonesia.or.id

Agha, S. Al. (2007). Money Laundering from Islamic Perspective, *10*(4), 406–411. https://doi.org/10.1108/13685200710830899

Akinbowale, Oluwatoyin E, Klingelhöfer, Heinz. E., & Zerihun, Mulatu. F. (2023). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*, 1–15. https://doi.org/10.1108/JFC-10-2022-0260

Al-Kaabi, S. S., & Belhaouari, S. B. (2019). Methods toward Enhancing RSA Algorithm: A Survey. *IJNSA*, *11*(3), 1-10. http://dx.doi.org/10.2139/ssrn.3412776

Ali, M. A., Hussinb, N., & Abed, I. A. (2019). E-Banking Fraud Detection: A Short Review. *International Journal of Innovation*, *6*(8), 67–87.

Anugrah Nasution. (2022). *Mantan Pimpinan Bank Syariah di Sumatera Utara Palsukan Dokumen, Sekarang Dijebloskan ke Penjara*. Tribun-Medan.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *JBE*, *18*(2), 185–195.

Asllani, Arben, Lari, Alireza, & Lari, Nasim. (2018). Strengthening information technology security through the failure modes and effects analysis approach. *International Journal of Quality Innovation*, *4*(5), 1-14. https://doi.org/10.1186/s40887-018-0025-1.

Ayyubi, S. Al. (2021). *Ini Awal Mula Kasus Korupsi Rp14,2 Miliar di BSM Sidoarjo*. Bisnis.Com. https://kabar24.bisnis.com/read/20210607/16/1402510/ini-awal-mula-kasus-korupsi-rp142-miliar-di-bank-syariah-mandiri-sidoarjo

Datau, Rivaldo. (2017). Penggelapan Dana Simpanan Nasabah Sebagai Kejahatan Perbankan. *Lex Privatum*, *5*(1), 113–119.

Dyer, Jeffrey. H., & Singh, Harbir. (1998). The Relational View: Cooperative Strategy and Sources of Interorganizational Competitive Advantage. *The Academy of Management Review*, *32*(4), 660–679. https://doi.org/10.2307/259056.

Faradiza, S. A. (2018). Fraud Pentagon dan Kecurangan Laporan Keuangan. *EkBis*, 2(1), 1–22. https://doi.org/10.14421/EkBis.2018.2.1.1060.

Ghoshal, Sumantra. (1987). Global strategy: An organizing framework. *Strategic Management Journal*, *8*(5), 425–440. https://doi.org/10.1002/smj.4250080503.

Hasan, M. R., & Suhermanto, S. (2021). *Keamanan Sistem Perangkat Lunak dengan Secure Software Development Lifecycle*. *12*(1), 88–101. http://dx.doi.org/10.47927/jikb.v12i1.95.

Hendrianto, S., Dara, N., & Masturo, M. (2023). Pengaruh Fraud Pentagon terhadap Financial Statement Fraud. *2023*, *5*(4), 15546–15558. https://doi.org/10.31004/joe.v5i4.2655.

Herlita, S., & Bayunitri, B. I. (2021). Pengaruh Pengendalian Internal Terhadap Pencegahan Kecurangan (Studi Kasus pada PT. Dirgantara Indonesia (Persero) Kota Bandung). *JABE*, *7*(1), 1805–1830. https://doi.org/10.33197/jabe.vol7.iss1.2021.628.

Hormati, G. A., Adechandra, D., & Pesudo, A. (2019). Pengaruh Tekanan, Kesempatan, Rasionalisasi dan Kemampuan Terhadap Kecenderungan Aparatur Sipil Negara dalam Melakukan Kecurangan Akuntansi Studi Empiris Satuan Kerja Perangkat Daerah Kabupaten Bolaang Mongondow Timur. *Jurnal Ilmiah Akuntansi Dan Humanika*, *9*(2), 172–190. https://doi.org/10.23887/jiah.v9i2.20583.

Isgiyata, J., Indayani, I., & Budiyoni, E. (2018). Studi Tentang Teori Gone dan Pengaruhnya Terhadap Fraud Dengan Idealisme Pimpinan Sebagai Variabel Moderasi: Studi pada Pengadaan Barang / Jasa di Pemerintahan. *JDAB*, *5*(1), 31–42. http://dx.doi.org/10.24815/jdab.v5i1.8253.

Kanika, & Singla, J. (2019). Online Banking Fraud Detection System: A Review. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(3), 959–962. https://doi.org/10.30534/ijatcse/2019/96832019.

Kismawadi, E. R., Muddatstsir, U. D. Al, & Hamid, A. (2020). *Fraud Pada Lembaga Keuangan Dan NonKeuangan*. Rajawali Pers.

Masriadi. (2019). *Kasus Pencurian di BSM Terungkap, Pelakunya Karyawan Sendiri*. Kompas.Com.

Muchlis, R. (2018). Analisis SWOT Financial Technology (Fintech) Pembiayaan Perbankan Syariah Di Indonesia (Studi Kasus 4 Bank Syariah Di Kota Medan). *At-Tawassuth*, *3*(2), 335–357. https://doi.org/10.30821/ajei.v1i1.2735.

Mugarza, I., Flores, Jose L., & Montero, Jose. L. (2020). Security Issues & Software Updates Management in the Industrial Internet of Things (IIoT) Era. *Sensors (Basel)*, *20*(24), 1–22. https://doi.org/10.3390/s20247160.

Mujiatun, S., Jasin, H., Fahmi, M., & Jufrizen, J. (2022). Model Financial Technology (Fintech) Syariah di Sumatera Utara. *Owner: Riset Dan Jurnal Akuntansi*, *6*(3), 2830–2839. https://doi.org/10.33395/owner.v6i3.893.

Munawarah, H., & Yusuf, M. (2022). *Bank Digital Syariah: Analisis Cyber Security Menurut Hukum Positif di Indonesia & Hukum Ekonomi Syariah* (Parman Komarudin (ed.)). PT. Borneo Development Project.

Newswire. (2021). *Kasus Dana Raib Rp20 Miliar di Bank Mega Syariah, Begini Kelanjutannya*. Bisnis.Com.

Noviatun, S., & Isfandayani. (2020). Analisis Implementasi Pencegahan Pencucian Uang Menggunakan Customer dan Enhaced Due Dilligence di BSM Jakarta. *PARADIGMA Journal of Science, Religion and Culture Studies*, *17*(1), 72–86. https://doi.org/10.33558/paradigma.v17i1.2298.

Reskia, & Sofie. (2022). Pengaruh Internal Audit, Anti Fraud Awareness, Komitmen Organisasi dan Budaya Organisasi Terhadap Pencegahan Fraud (Studi kasus PT. Inti Persada Nusantara). *JET*, *2*(2), 419–432. https://doi.org/10.25105/jet.v2i2.14531.

Siregar, L. (2020). Review Pengujian Keamanan Perangkat Lunak dalam Software Development Life Cycle (SDLC). *ASEECT*, *3*(1), 1–11. http://doi.org/10.30871/aseect.v1i3.2380.

Sudarmanto, E., & Utami, C. K. (2021). Pencegahan Fraud Dengan Pengendalian Internal Dalam Perspektif Alquran. *JIEI*, *7*(1), 195–208. https://doi.org/10.29040/jiei.v7i1.1593.

Sumandi. (2017). Analisis Sistem Deteksi Dini Terhadap Krisis Perbankan Syariah. *Nisbah*, *3*(1), 365–381. https://doi.org/10.30997/jn.v3i1.784.

Tsabita, A. W. Z., Fanfa, H. S., & Syahada, M. R. (2023). Systematic Literature Review (SLR): Standar Manajemen Keamanan Sistem Perbankan. *Journal Central Publisher*, *1*(4), 310–327.

Vona, L. W. (2012). *Fraud Risk Assessment: Building a Fraud Audit Program*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781119196655.

Williamson, O. E. (1979). Transaction-Cost Economics : The Governance of Contractual Relations. *Journal of Law and Economics*, *22*(2), 233–261.

Zulkarnain, & Sutabri, T. (2023). Analisis Kejahatan Carding pada BNI 46. *Blantika: Multidisciplinary Journal*, *2*(1), 33–43. https://doi.org/10.57096/blantika.v2i1.10.