IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Volume 6, Issue 2, July 2025, 80-90

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.ac.id

Can Indonesia's Digital Banks COMbat PEPs and Financial Crimes?

Anang Riyan Ramadianto[1], Dharma Setiawan Negara[2], Chita Askarya[3], Larmi Kristiani[4]
[1]Faculty of Law Universitas Brawijaya, Indonesia
[2]Faculty of Law and Social Sciences Universitas Sunan Giri Surabaya, Indonesia
[3]AML/CFT SeaBank Indonesia
[4]The Supreme Court of The Republic of Indonesia.
Email : anangramadian@student.ub.ac.id

Submitted: 26-02-2025; Reviewed: 26-07-2025; Revised:30-07-2025; Accepted: 31-07-2025
DOI: https://doi.org/10.18196/ijclc.v6i2.26038

Abstract

This article examines the impact of advanced technologies on enhancing due diligence for Politically Exposed Persons (PEPs) within Indonesia's digital banking sector. With the rapid growth of digital banking, there is a pressing need to address the heightened risks associated with PEPs, including potential corruption and money laundering. The study explores the challenges posed by traditional due diligence methods in the face of evolving financial technologies like artificial intelligence (AI) and machine learning (ML), which offer innovative solutions to improve compliance and risk management. It emphasizes the importance of robust regulatory frameworks designed to safeguard the financial system, while also highlighting the operational realities faced by digital banks in adhering to these regulations. The research employs qualitative analysis to investigate how technology can streamline compliance processes, enhance customer due diligence (CDD), and facilitate the identification and monitoring of high-risk clients. Additionally, it discusses the implications of these technological advancements for both regulatory compliance and overall financial security in Indonesia. By focusing on the intersection of technology, regulation, and compliance challenges, this study underscores the critical role of digital banking in mitigating financial crime risks associated with PEPs in an increasingly complex financial landscape.

Keywords: Digital Banking; Due Diligence; Politically Exposed Persons (PEPs)

I. Introduction

In recent years, the financial landscape has undergone a dramatic transformation due to the rise of digital banking, which offers unprecedented convenience and accessibility to consumers.[1] This innovation, while beneficial, has also introduced significant challenges, particularly in managing financial crime risks.[2] As digital banks continue to proliferate, understanding the unique dynamics of financial crime associated with Politically Exposed Persons (PEPs) becomes crucial for safeguarding the integrity of financial systems.[3] PEPs, defined as individuals who hold prominent public positions or roles in government, often present elevated risks due to their potential for involvement in corrupt practices and financial crimes.[4] The global nature of banking facilitates the movement of criminal proceeds across jurisdictions, allowing illicit activities to exploit banking systems, especially those lacking robust regulatory frameworks.[5] Consequently, digital banks have become attractive targets for financial criminals, making it

[1] Alla Klimenko, "Digital Transformation in Banking and Financial Services," *Mad Devs*, September 24, 2024, https://maddevs.io/blog/digital-transformation-in-banking-and-financial-services/.

[2] Ahmad Mushtaq, "Compliance Challenges and Tech-Driven Solutions in Combating Financial Crime Within the Fintech Ecosystem," *Lovely Professional University* 4, no. 1 (May 2024): 62–80, https://doi.org/DOI:10.4018/979-8-3693-3633-5.ch005.

[3] Steven Beck et al., "Financial Crimes Compliance: The Power of Partnership," ADB Briefs, 0 ed., ADB Briefs (Manila, Philippines: Asian Development Bank, July 2021), https://doi.org/10.22617/BRF210250-2.

[4] Theodore S Greenberg, *Politically Exposed Persons Preventive Measures For The Banking Sector* (Washington: The International Bank for Reconstruction and Development / The World Bank, 2010), DOI: 10.1596/978-0-8213-8249-3.

[5] UNCTAD, ed., *Tackling Illicit Financial Flows for Sustainable Development in Africa*, Economic Development in Africa Report 2020 (Geneva: United Nations, 2020).

imperative for these institutions to develop effective strategies to mitigate associated risks.[6]

Indonesia has seen rapid growth in digital banking, spurred by high smartphone penetration, shifting consumer preferences for convenient financial services, and government support for financial inclusion such as SeaBank, Bank Jago, Jenius, and etc.[7] Both traditional banks and fintech startups have responded to this demand, launching digital banks that offer fast, user-friendly financial services. In response to this growth, the Financial Services Authority of Indonesia (OJK) has issued regulations to support and guide digital banking development.[8] Notably, OJK Regulation No. 12/POJK.03/2021[9] sets operational standards, including requirements around capital, data security, and customer protection, which help digital banks maintain anti-money laundering (AML) and counter-terrorism financing (CTF) compliance. This framework supports digital banks in managing some of the risks associated with online financial platforms.

In this regulatory context, numerous studies underscore the complex intersection of digital banking, financial crime, and PEPs. For instance, Mushtaq[10] et al. (2024) highlight compliance challenges faced by fintech firms in preventing financial crime, emphasizing technology-driven solutions like artificial intelligence, machine learning, and blockchain to enhance security and streamline compliance. These tools aid in detecting fraud more effectively and securing data privacy, strengthening the fintech sector's defenses against illicit activities. However Theodore[11] (2010) addresses best practices for identifying and managing PEPs, who, because of their influence, are susceptible to corrupt practices. Theodore stresses the importance of regulatory compliance, due diligence, and risk assessment strategies to protect banking systems. Yet despite extensive literature, a gap remains in how digital banks can tailor their risk management frameworks to meet the unique challenges posed by PEPs. This study aims to bridge that gap by examining best practices for mitigating financial crime risks in digital banking.

According to 2024 financial reports covered by *Finansial Bisnis*[12], the digital banks with the largest assets in Indonesia include Seabank, leading with assets of IDR 32.34 trillion, a slight decrease from IDR 32.72 trillion in 2023, and Bank Jago with IDR 22.5 trillion, reflecting significant growth from IDR 18.02 trillion. Bank Neo Commerce reports IDR 18.91 trillion in assets, slightly lower than the previous year. Hibank has shown strong growth, with assets rising to IDR 15.14 trillion from IDR 11.63 trillion, followed by BCA Digital (blu) with an increase to IDR 14.34 trillion, and Allo Bank with assets of IDR 12.74 trillion. Bank Raya's assets, however, experienced a minor decline to IDR 12.24 trillion from IDR 12.64 trillion.

In managing financial crime risks, Indonesia's legal frameworks play a crucial role, particularly in AML and CTF measures. Important regulations include Law No. 8 of 2010 on Money Laundering Prevention and Law No. 9 of 2013 on Terrorism Financing Prevention, as well as OJK Regulation No. 8 of 2023, which mandates AML and CTF compliance for financial institutions.[13] To counter risks associated with easy

[6] Abdulbasit A. Darem et al., "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," *IEEE Access* 11 (2023): 125138–58, https://doi.org/10.1109/ACCESS.2023.3327016.

[7] Sumit Kumar, "Indonesia's Fintech Industry Is Ready to Rise" (Indonesia, March 2023).

[8] Santoso Wimbah, "Financial Services Authority to Improve Digitalization of Financial Sector," *Cabinet Secretariat of The Republic of Indonesia* 1, no. 1 (2021): 1–2, https://setkab.go.id/en/financial-services-authority-to-improve-digitalization-of-financial-sector/.

[9] See Article 30 of the regulation states that Bank BHI, which operates as a digital bank, must comply with all applicable legal regulations for Bank BHI. This means that Bank BHI is required to adhere to all banking regulations, including legal provisions, those set forth by the Financial Services Authority (OJK), and other policies applicable to digital banks. In other words, even though Bank BHI operates digitally, it must maintain the same compliance requirements as conventional banks regarding capital adequacy, data protection, cybersecurity, anti-money laundering (AML), and counter-terrorism financing (CTF). This provision emphasizes that the form of digitalization does not lessen compliance responsibilities but rather requires equivalent or higher standards in addressing the unique risks faced by digital banks.

[10] Mushtaq, "Compliance Challenges and Tech-Driven Solutions in Combating Financial Crime Within the Fintech Ecosystem."

[11] Greenberg, *Politically Exposed Persons Preventive Measures For The Banking Sector*.

[12] Arlina Laras, "Top 7 Bank Digital Di Indonesia Kuartal I/2024: Seabank Teratas, Hibank Melesat," 2024, https://finansial.bisnis.com/read/20240525/90/1768141/top-7-bank-digital-di-indonesia-kuartal-i20.

[13] Shelvi Rusdiana, "Rethinking Indonesian Anti-Money Laundering Laws in the Age of Online Gaming Economies," *NURANI: JURNAL KAJIAN SYARI'AH DAN MASYARAKAT* 24, no. 2 (October 23, 2024): 360–74, https://doi.org/10.1910 9/nurani.v24i2.24422.

account-opening processes, digital banks in Indonesia perform Customer Due Diligence (CDD) as required by OJK Regulation No. 8 of 2023.[14] CDD encompasses comprehensive customer identification, covering personal details, beneficial ownership, funding sources, and transaction purposes.[15] For PEPs, who are deemed high-risk clients, Enhanced Due Diligence (EDD) is mandated, involving rigorous scrutiny of customer relationships to protect against financial crime. The Managing Financial Crime Risk (MFCR) framework outlined in POJK 12/2017 further supports digital banks in identifying, assessing, monitoring, and escalating risks when unusual activities are detected.

This study seeks to address the central question: *How can Indonesia digital banks effectively manage financial crime risks associated with Politically Exposed Persons (PEPs)?* Through normative legal research and case studies of leading digital banks with successful PEP risk management practices, this research explores potential solutions, including advanced risk assessment frameworks, enhanced due diligence, and transaction monitoring technologies. By investigating these strategies, this study aims to provide insights into effective approaches for digital banks in mitigating financial crime risks posed by PEPs, ultimately contributing to a stronger, more secure financial system in Indonesia and beyond.

II. Metode Penelitian

This research adopts a normative legal research approach, focusing on the legal frameworks, regulations, and practices involved in managing financial crime risks, specifically related to Politically Exposed Persons (PEPs) in Indonesia's digital banking sector. The study employs a qualitative method, relying on secondary data sources including regulatory documents, literature reviews, financial reports, and case studies of digital banks operating in Indonesia. The research aims to analyze how digital banks implement due diligence processes and utilize technology to mitigate risks associated with PEPs.

III. Result and Discussion

A. The Role of Technology in Enhancing Due Diligence for PEPs in Indonesia

The rise of digital banking in Indonesia has brought forth unique challenges in terms of financial oversight, transparency, and regulation, particularly in the management of high-risk clients, such as Politically Exposed Persons (PEPs).[16] Given the risks associated with PEPs, including possible corruption, financial misconduct, or involvement in money laundering, enhanced due diligence has become a critical area of focus for banks and regulatory bodies in Indonesia. The evolving landscape of financial technology, encompassing artificial intelligence (AI), machine learning (ML), and blockchain, has become indispensable in supporting due diligence processes, ensuring financial integrity, and reducing the risk of financial crime.[17] This part will discuss how these technologies enhance due diligence for PEPs in the Indonesian banking system, focusing on the mechanisms, applications, and challenges associated with digital banking compliance.

Politically Exposed Persons are individuals who hold significant roles in public office, government, or military sectors or are otherwise affiliated with influential organizations.[18] Their positions inherently increase their risk of being involved in illicit financial activities due to the power and access they wield. PEPs may leverage their influence for personal gain, which could involve hiding assets, engaging in

[14] Otoritas Jasa Keuangan, *Indonesia Banking Booklet 2023*, 10th ed. (Jakarta, Indonesia: Otoritas Jasa Keuangan Department of Banking Licensing and Crisis Management, 2023).

[15] Bank Negara Malaysia, “Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT/CPF and TFS for FIs),” *Central Bank of Malaysia*, February 5, 2024, 1–175.

[16] Wardah Yuspin et al., “Personal Data Protection Law in Digital Banking Governance in Indonesia,” *Studia Iuridica Lublinensia* 32, no. 1 (March 28, 2023): 99–130, https://doi.org/10.17951/sil.2023.32.1.99-130.

[17] Ganda Raharja Rusli and Anestia Hayubriandini Fermay, “Digital Financial Services Effort in Enforcing Anti-Money Laundering through Open Banking Optimization,” *AML/CFT Journal The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 2 (June 1, 2024): 159–74, https://doi.org/10.59593/amlcft.2024.v2i2.158.

[18] Guillermo Jorge, “Identification and Exchange of Information on Politically Exposed Persons in Central American Countries” (Inter-American Development Bank, August 3, 2018), https://doi.org/10.18235/0010714.

unauthorized transactions, or manipulating financial flows.[19] Due to this potential for abuse, PEPs are regarded as high-risk clients, and regulatory frameworks worldwide require banks to implement stricter oversight measures for PEP transactions.

Banks must proactively manage these risks by conducting thorough due diligence on PEP clients. This includes not only understanding the individual's background, sources of funds, and affiliations but also monitoring for any anomalous activity in their financial transactions. Traditional methods of due diligence, however, are proving inadequate in keeping up with the speed and complexity of transactions in digital banking. This has given rise to a critical need for technology-driven solutions to support risk management and compliance efforts.

Within the framework of banking compliance, Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) serve as foundational processes for identifying and assessing client risks.[20] CDD involves verifying client identities, understanding their risk profiles, and establishing basic parameters for transaction monitoring. EDD, on the other hand, is a more rigorous process reserved for high-risk clients, particularly PEPs. It involves deeper analysis, continuous monitoring, and more frequent reviews of transactions to detect suspicious patterns indicative of financial misconduct[21].

The distinction between CDD and EDD lies in the intensity of the oversight, with EDD incorporating more comprehensive checks and often employing specialized technology for effective risk mitigation.[22] For banks in Indonesia, ensuring that EDD measures are both effective and efficient is paramount, as they must balance the demand for swift, accessible digital banking services with the need for transparency and regulatory compliance.

Money laundering is one of the principal financial crimes linked to PEPs, and understanding this process is key to recognizing the risks involved.[23] Money laundering refers to the act of concealing illicitly acquired funds to make them appear legitimate. Predicate offenses, or the original criminal acts that generate these funds, can vary widely, encompassing corruption, drug trafficking, bribery, and even cybercrime. Money laundering typically occurs in three stages: placement, layering, and integration. In the placement phase, criminals introduce proceeds of crime into the financial system; in the layering phase, they obscure the funds' origins through complex transactions, and in the integration phase, they reinvest the laundered funds into the legitimate economy.[24]

For banks in Indonesia, where digital transactions have become increasingly rapid and accessible, monitoring and detecting money laundering schemes has become significantly more complex.[25] Advanced technologies, such as AI and blockchain, can assist in identifying irregular patterns in transaction flows, providing a more efficient solution than traditional manual checks. These technological innovations enable digital banks to enhance their risk assessment processes, giving them a competitive edge in combatting financial crimes.[26]

[19] Muhammad Burhanudin Arifin and Andrian Budi Prasetyo, "Factors Influencing in the Fraudulent Financial Reporting" 10, no. 2 (2018).

[20] Munachi Ijeoma Ononiwu, Obianuju Clement Onwuzulike, and Kazeem Shitu, "Comparative Analysis of Customer Due Diligence and Compliance: Balancing Efficiency with Regulatory Requirements in the Banking Sectors of the United States and Nigeria," *World Journal of Advanced Research and Reviews* 23, no. 3 (September 30, 2024): 475–91, https://doi.org/10.30574/wjarr.2024.23.3.2707.

[21] Norman Mugarura, "Customer Due Diligence (CDD) Mandate and the Propensity of Its Application as a Global AML Paradigm," *Journal of Money Laundering Control* 17, no. 1 (January 7, 2014): 76–95, https://doi.org/10.1108/JMLC-07-2013-0024.

[22] Howard Chitimira and Sharon Munedzi, "Overview International Best Practices on Customer Due Diligence and Related Anti-Money Laundering Measures," *Journal of Money Laundering Control* 26, no. 7 (December 18, 2023): 53–62, https://doi.org/10.1108/JMLC-07-2022-0102.

[23] Patience Okpeke Paul and Toluwalase Vanessa Iyelolu, "Anti-Money Laundering Compliance and Financial Inclusion: A Technical Analysis of Sub-Saharan Africa," *GSC Advanced Research and Reviews* 19, no. 3 (June 30, 2024): 336–43, https://doi.org/10.30574/gscarr.2024.19.3.0235.

[24] Erik Altman et al., "Realistic Synthetic Financial Transactions for Anti-Money Laundering Models," n.d.

[25] Agus Joko Lelono, Mohamad Tohari, and Hono Sejati, "The Urgency of Legal Reform for the Legality of Digital Currency in Indonesia" 6, no. 4 (2024).

[26] Irshad Ahmed Hashimzai and Mohammad Zameer Ahmadzai, "Navigating the Integration of Blockchain Technology in Banking: Opportunities and Challenges," *International Journal Software Engineering and*

The compliance function within banks plays a pivotal role in monitoring adherence to regulations and identifying potential financial risks, particularly concerning PEPs. Compliance teams are responsible for ensuring that all activities involving PEPs are in line with regulatory standards and that they exhibit no signs of suspicious transactions. Banks that fail to enforce adequate compliance measures risk regulatory penalties, reputational damage, and a loss of client trust. For digital banks in Indonesia, compliance is not only a regulatory requirement but also a strategic advantage that can enhance customer confidence and loyalty.

In recent years, digital banks such as Seabank and Jenius have prioritized the integration of advanced compliance technologies to streamline their due diligence processes. Through the application of AI and ML, these banks have automated significant aspects of client verification, risk scoring, and anomaly detection. HSBC has gone a step further, employing Google Cloud's AML (Anti-Money Laundering) AI, a sophisticated system designed to accelerate anomaly detection, expedite investigations, and support compliance with the use of high-performance computing on the cloud. This system illustrates how leveraging advanced compliance technologies can help banks achieve more accurate and timely financial crime prevention.[27]

Screening PEPs involves gathering detailed data on clients to ensure that they are appropriately classified and monitored. Banks typically collect information on a PEP's sources of funds, political connections, and affiliations, which is then analyzed to detect any patterns indicative of illegal activity. The implementation of AI has significantly enhanced this process, allowing banks to conduct real-time analysis of client data and respond more effectively to potential threats. Digital banks can now leverage AI's data-processing capabilities to continuously monitor transaction activity, analyzing both structured and unstructured data to gain a more comprehensive understanding of client behavior.

In addition to identifying suspicious patterns, AI also aids in risk assessment by generating risk scores for clients. This capability allows banks to assign levels of risk to each PEP based on transaction histories, types of transactions, and even external factors like regional geopolitical dynamics. With this information, banks can apply tailored compliance measures, scaling their response according to the severity of the risk.

Effective risk management for PEPs requires a systematic approach that balances transparency and operational efficiency. Banks typically begin by establishing a detailed risk profile for each PEP, gathering relevant data to determine their level of exposure to financial crime. Continuous surveillance follows, with automated systems monitoring for irregularities in transaction patterns. When suspicious transactions are detected, banks are obligated to report these to the appropriate regulatory authorities in Indonesia, this involves submitting reports to the Financial Transaction Reports and Analysis Center (PPATK).[28]

Technologies like Seabank's seamless AI-powered systems and HSBC's AML AI solution are highly effective in managing these tasks, allowing banks to monitor high transaction volumes while maintaining a high level of accuracy. HSBC's AML AI system, hosted on Google Cloud, exemplifies how AI-driven financial crime detection can be refined over time through continuous feedback loops. These systems analyze investigation outcomes to adjust their detection models, increasing the model's accuracy and responsiveness to emerging threats.[29]

AI-driven risk detection operates through a multi-stage process, with data preparation being the first step. Here, transaction data, account histories, and customer profiles are gathered and processed to create a structured dataset for analysis. The AI model then applies machine learning algorithms to detect patterns that indicate potential financial crimes. When the system identifies a risk, it generates a risk score that is accompanied by an "explainability" feature, which outlines the rationale behind the score. This explainability helps compliance teams understand the factors driving the risk, making it easier to prioritize

Computer Science (IJSECS) 4, no. 2 (August 10, 2024): 665–79, https://doi.org/10.35870/ijsecs.v4i2.2656.

[27] Google Cloud, "Fighting Money Launderers with Artificial Intelligence at HSBC," *Google Cloud Blog FInancial Seervices* 1, no. 1 (November 30, 2023): 1–3, https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence.

[28] Fajar Sugianto and Joshua Evandeo Irawan, "Urgensi Menjadikan Hasil Analisis (HA)/Hasil Pemeriksaan (HP) PPATK Sebagai Alat Bukti Dalam Perkara TPPU Dan TPPT Di Indonesia," *AML/CFT Journal The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 2 (June 1, 2024): 147–58, https://doi.org/10.59593/amlcft.2024.v2i2.153.

[29] Cloud, "Fighting Money Launderers with Artificial Intelligence at HSBC."

cases that require further investigation.

Following the scoring process, compliance teams review flagged cases according to the bank's risk tolerance. If further investigation is required, the AI model's explainability feature guides investigators, offering insights into the flagged transactions' nature. Finally, a dynamic feedback loop allows the AI model to continuously refine its detection algorithms, adapting to new patterns of financial crime over time.

When a PEP client is implicated in criminal activities, banks have a duty to report these findings to regulatory authorities. Before filing such a report, however, the bank must conduct a thorough investigation to gather sufficient evidence. AI expedites this process by facilitating the collection and analysis of digital evidence, which can significantly reduce the time needed to confirm suspicious activities. If the investigation substantiates the allegations, the bank may take appropriate actions, such as account suspension or service limitations, to prevent further illicit activity.

The Indonesian financial sector has made substantial progress in adopting technology-based solutions to enhance the due diligence processes for PEPs. By effectively utilizing AI, ML, and blockchain, digital banks are better equipped to detect, prevent, and report financial crime in an increasingly complex regulatory environment. However, the implementation of these advanced technologies is not without challenges. For smaller digital banks, in particular, the cost of adopting high-quality AI systems and the need for large, structured datasets may pose limitations. High-quality data is crucial for AI accuracy, and in emerging markets with limited data-sharing frameworks, access to such data can be challenging.

The adoption of advanced technology for due diligence processes brings significant benefits, but it also introduces certain challenges. Smaller digital banks in Indonesia may find the investment costs associated with AI and ML systems prohibitive. Additionally, the accuracy of AI and ML models is highly dependent on data quality, which may be harder to obtain in regions where data-sharing frameworks are underdeveloped. Therefore, while technology enhances due diligence capabilities, it also requires banks to carefully balance

B. Regulatory Frameworks and Compliancce Challenges for Digital Banks

The rise of digital banking in Indonesia has transformed the financial services landscape, offering unprecedented convenience and accessibility to consumers.[30] With the rapid adoption of technology, digital banks have emerged to meet the growing demand for seamless banking experiences.[31] However, this evolution has also introduced significant challenges, particularly in terms of compliance with regulatory frameworks designed to combat financial crime. Understanding the interplay between regulations and the operational realities of digital banking is crucial for mitigating risks associated with money laundering and terrorist financing, especially concerning Politically Exposed Persons (PEPs).[32]

In Indonesia, the regulatory framework for digital banks is primarily governed by the Financial Services Authority (OJK), which has established a series of regulations aimed at ensuring the integrity of the financial system.[33] Notable among these regulations is OJK Regulation No. 12/POJK.03/2021, which sets operational standards for digital banks, including requirements for capital adequacy, data security, and customer protection.[34] This regulation mandates that digital banks develop robust risk management frameworks that align with anti-money laundering (AML) and counter-terrorism financing (CTF) measures. Additionally, Law No. 8 of 2010 on the Prevention of Money Laundering outlines the legal obligations for financial institutions to implement effective AML strategies, emphasizing the importance of conducting thorough Customer Due Diligence (CDD). This is complemented by Law No. 9 of 2013 on the

[30] Luiz Antonio Bueno et al., "Impacts of Digitization on Operational Efficiency in the Banking Sector: Thematic Analysis and Research Agenda Proposal," *International Journal of Information Management Data Insights* 4, no. 1 (April 2024): 100230, https://doi.org/10.1016/j.jjimei.2024.100230.

[31] Chitra Laksmi Rithmaya, Herwin Ardianto, and Evi Sistiyarini, "GEN Z AND THE FUTURE OF BANKING: AN ANALYSIS OF DIGITAL BANKING ADOPTION," *Jurnal Manajemen Dan Kewirausahaan* 26, no. 1 (March 1, 2024): 64–78, https://doi.org/10.9744/jmk.26.1.64-78.

[32] Jamal Wiwoho, Dona Budi Kharisma, and Dwi Tjahja K. Wardhono, "Financial Crime In Digital Payments," *Journal of Central Banking Law and Institutions* 1, no. 1 (December 28, 2021): 47–70, https://doi.org/10.21098/jcli.v1i1.7.

[33] Assegaf Hamzah Partners, "OJK Embraces Digital Bank with New Regulations," *Rajah & Tann Asia Lawyers Who Know Asia* 1, no. 1 (November 2021): 1–6, https://www.ahp.id/clientalert/AHPClientUpdate-4November2021.pdf.

[34] Evita Isretno Israhadi, "Review of Digital Bank Law in Indonesia: Challenges in the Digital Era," n.d.

Prevention of Terrorism Financing, which establishes protocols for identifying and mitigating risks associated with terrorist financing activities. Further regulatory guidance is provided by OJK Regulation No. 8 of 2023, which details the CDD processes that digital banks must adhere to. This regulation highlights the necessity for Enhanced Due Diligence (EDD) for high-risk clients, including PEPs, requiring banks to conduct a more in-depth analysis of these clients' backgrounds, source of funds, and transactional patterns.

The regulatory framework aims to establish a solid foundation for digital banks to operate securely while safeguarding against illicit financial activities. However, the practical implementation of these regulations poses several compliance challenges. Digital banks operate in a fast-paced technological environment where innovations frequently outpace regulatory adaptations. The challenge for banks lies in balancing the implementation of cutting-edge technologies with adherence to existing regulations. Many digital banks may find it difficult to ensure compliance with AML requirements while simultaneously leveraging technology to enhance customer experience. For instance, the use of automated systems for onboarding clients must still comply with KYC requirements, necessitating ongoing adjustments to their compliance frameworks.[35]

One of the most significant challenges digital banks face is the identification and ongoing monitoring of PEPs. PEPs are individuals who hold prominent public positions and may present higher risks due to their potential involvement in corrupt practices. The criteria for defining PEPs can vary across jurisdictions, complicating the identification process for banks operating in a globalized economy. Digital banks must implement comprehensive screening processes to identify PEPs accurately, which requires access to reliable databases and continuous monitoring systems. Furthermore, maintaining updated records of clients' political connections and risk factors is resource-intensive, often stretching the capabilities of smaller banks. Digital banks collect extensive personal and financial data to comply with CDD regulations. However, the intersection of data privacy laws and AML regulations creates a complex compliance landscape. In Indonesia, the ITE Law governs electronic transactions and data protection, mandating that banks protect customer information. Compliance with both the ITE Law and AML regulations can be challenging, particularly when implementing measures for data sharing and transparency required for effective CDD. Digital banks must navigate the risks of data breaches while fulfilling their regulatory obligations, necessitating a robust data governance framework.[36]

While advanced compliance technologies, such as AI and machine learning, can enhance a bank's ability to detect suspicious activities, the financial burden of implementing these systems can be significant. Smaller digital banks may struggle to allocate sufficient resources for technology investments needed for effective compliance.[37] High initial costs and ongoing maintenance expenses can create disparities between larger institutions that can afford comprehensive compliance solutions and smaller fintech companies that may lack the necessary funding. Fostering a culture of compliance within digital banks is essential for effective risk management.[38] However, employees may resist compliance initiatives, viewing them as added burdens rather than integral to the organization's success. Building a compliance-oriented culture requires ongoing education and training programs that emphasize the importance of regulatory adherence. Without strong buy-in from all levels of the organization, compliance efforts can falter, leaving banks vulnerable to regulatory breaches.

The regulatory landscape in Indonesia is continually evolving, with frequent updates and changes to existing regulations. Digital banks must remain agile in their compliance efforts to adapt to these changes promptly.[39] The lack of clear guidance on certain regulatory aspects can create uncertainty, making it challenging for banks to implement compliant practices confidently. Staying informed about regulatory updates and interpreting their implications for business operations are critical components of effective

[35] Rusli and Fermay, "Digital Financial Services Effort in Enforcing Anti-Money Laundering through Open Banking Optimization."

[36] Moch Syahren Lazuardy et al., "Legal Framework for Protecting Bank Customers against Personal Data Leakage in the Digital Era: A Study of Indonesian Regulations," *Indonesian Journal of Multidisciplinary Science* 3, no. 10 (July 25, 2024), https://doi.org/10.55324/ijoms.v3i10.907.

[37] Beatrice Oyinkansola Adelakun et al., "Enhancing Fraud Detection in Accounting through AI: Techniques and Case Studies," *Finance & Accounting Research Journal* 6, no. 6 (June 15, 2024): 978–99, https://doi.org/10.51594/farj.v6i6.1232.

[38] Douglas W. Arner, Janos Nathan Barberis, and Ross P. Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm?," *SSRN Electronic Journal*, 2015, https://doi.org/10.2139/ssrn.2676553.

[39] Partners, "OJK Embraces Digital Bank with New Regulations."

compliance strategies.

To illustrate how digital banks in Indonesia are managing compliance challenges, it is beneficial to examine specific examples of successful practices and strategies. Seabank, one of Indonesia's leading digital banks, has implemented a comprehensive compliance program to address regulatory requirements and manage financial crime risks. Recognizing the complexities of identifying PEPs, Seabank has invested in advanced screening technologies that utilize machine learning algorithms to analyze customer data and flag potential high-risk clients. This proactive approach enables Seabank to enhance its CDD processes, ensuring that it meets the stringent requirements set forth by OJK regulations. Moreover, Seabank has established a dedicated compliance team responsible for monitoring regulatory changes and ensuring that the bank's policies are aligned with evolving requirements. Regular training sessions are conducted for employees to instill a culture of compliance, emphasizing the importance of adhering to AML and CTF protocols. To address data privacy concerns, Seabank has implemented strict data governance policies that comply with both AML regulations and data protection laws. By prioritizing data security, the bank enhances customer trust while meeting regulatory obligations.

Bank Jago is another example of a digital bank successfully navigating the regulatory landscape in Indonesia. The bank has embraced digital technology to streamline its compliance processes, utilizing automated systems for real-time monitoring of transactions. By leveraging AI and big data analytics, Bank Jago can identify unusual transaction patterns quickly, enabling rapid response to potential risks. To mitigate the challenges associated with identifying PEPs, Bank Jago has established partnerships with external data providers to enhance its screening capabilities. This collaboration ensures that the bank has access to up-to-date information on political connections, allowing for more accurate risk assessments. Furthermore, Bank Jago has prioritized employee training and awareness programs, fostering a culture of compliance across the organization. The bank's commitment to regulatory adherence is reflected in its comprehensive compliance framework, which emphasizes transparency and accountability.

Digital banks in Indonesia can strengthen their compliance frameworks by prioritizing investments in compliance technologies that enhance operational efficiency and ensure adherence to regulatory requirements. Utilizing AI and machine learning can automate monitoring processes, allowing banks to detect suspicious activities more effectively. Additionally, investing in secure data management systems will help protect customer information while complying with data privacy regulations. Establishing a robust training program for staff is crucial for fostering a compliance-oriented culture. Regular training sessions on regulatory requirements, risk management, and the importance of compliance will equip employees with the knowledge needed to navigate complex compliance landscapes. Encouraging a culture of transparency and accountability will further strengthen compliance efforts across the organization.

Digital banks should refine their risk assessment frameworks to incorporate both quantitative and qualitative measures for evaluating client risks, particularly for PEPs. Developing comprehensive profiles that consider various risk factors will enable banks to tailor their due diligence efforts and ensure appropriate monitoring of high-risk clients. Maintaining open lines of communication with regulatory authorities can help digital banks stay informed about regulatory changes and expectations. Participating in industry forums and engaging in collaborative initiatives can facilitate information sharing and promote best practices for compliance. Digital banks must develop well-documented policies and procedures outlining compliance obligations and processes. This includes comprehensive guidelines for CDD, EDD, and ongoing monitoring of client relationships. A clear compliance framework will help ensure consistency in practices across the organization and reduce the risk of regulatory breaches. Collaborating with external compliance experts can provide valuable insights and resources to strengthen compliance programs. Digital banks may consider outsourcing certain compliance functions to specialized firms that can help navigate the complexities of regulatory compliance while managing costs effectively.

The regulatory frameworks governing digital banks in Indonesia are essential for safeguarding the integrity of the financial system and mitigating risks associated with financial crimes, particularly concerning PEPs. However, the challenges posed by rapid technological changes, data privacy concerns, and the dynamic regulatory environment necessitate that digital banks adopt proactive compliance strategies. By investing in technology, fostering a culture of compliance, and refining risk assessment frameworks, digital banks can effectively navigate the complexities of regulatory compliance. Continued collaboration with regulatory authorities and industry peers will further enhance the compliance capabilities of digital banks, contributing to a more secure and resilient financial ecosystem in Indonesia.

IV. Conclusion

The examination of the role of technology in enhancing due diligence for Politically Exposed Persons (PEPs) in Indonesia highlights the critical need for financial institutions to adopt innovative solutions in response to the evolving challenges of digital banking. Findings indicate that leveraging advanced technologies such as artificial intelligence and machine learning significantly improves the ability of banks to conduct real-time monitoring and risk assessment. These technologies enable banks to efficiently analyze vast amounts of data, facilitating the identification of suspicious activities that may indicate financial misconduct. The implementation of Enhanced Due Diligence (EDD) protocols further reinforces the importance of thorough risk management, allowing banks to maintain compliance with regulatory standards while offering competitive services.

The regulatory landscape established by the Financial Services Authority (OJK) underscores the necessity for digital banks to navigate complex compliance requirements effectively. The challenges posed by rapid technological advancements and evolving regulatory frameworks necessitate that banks develop adaptive compliance strategies. Recommendations include investing in robust compliance technologies, fostering a culture of regulatory adherence among staff, and establishing comprehensive risk assessment protocols for PEPs. By prioritizing these initiatives, digital banks can enhance their due diligence processes, minimize the risks associated with financial crime, and ultimately contribute to a more resilient financial ecosystem in Indonesia. The implications of these findings suggest that a proactive approach to compliance, coupled with the strategic use of technology, will be vital for digital banks in addressing the challenges presented by high-risk clients.

Bibliography

Altman, Erik, Jovan Blanuša, Béni Egressy, Andreea Anghel, and Kubilay Atasu. “Realistic Synthetic Financial Transactions for Anti-Money Laundering Models,” n.d.

Arifin, Muhammad Burhanudin, and Andrian Budi Prasetyo. “Factors Influencing in the Fraudulent Financial Reporting” 10, no. 2 (2018).

Arner, Douglas W., Janos Nathan Barberis, and Ross P. Buckley. “The Evolution of Fintech: A New Post-Crisis Paradigm?” *SSRN Electronic Journal*, 2015. https://doi.org/10.2139/ssrn.2676553.

Beatrice Oyinkansola Adelakun, Ebere Ruth Onwubuariri, Gbenga Adeniyi Adeniran, and Afari Ntiakoh. “Enhancing Fraud Detection in Accounting through AI: Techniques and Case Studies.” *Finance & Accounting Research Journal* 6, no. 6 (June 15, 2024): 978–99. https://doi.org/10.51594/farj.v6i6.1232.

Beck, Steven, Lotte Schou-Zibell, Can Sutken, and Catherine Estrada. “Financial Crimes Compliance: The Power of Partnership.” ADB Briefs. 0 ed. ADB Briefs. Manila, Philippines: Asian Development Bank, July 2021. https://doi.org/10.22617/BRF210250-2.

Bueno, Luiz Antonio, Tiago F.A.C. Sigahi, Izabela Simon Rampasso, Walter Leal Filho, and Rosley Anholon. “Impacts of Digitization on Operational Efficiency in the Banking Sector: Thematic Analysis and Research Agenda Proposal.” *International Journal of Information Management Data Insights* 4, no. 1 (April 2024): 100230. https://doi.org/10.1016/j.jjimei.2024.100230.

Chitimira, Howard, and Sharon Munedzi. “Overview International Best Practices on Customer Due Diligence and Related Anti-Money Laundering Measures.” *Journal of Money Laundering Control* 26, no. 7 (December 18, 2023): 53–62. https://doi.org/10.1108/JMLC-07-2022-0102.

Cloud, Google. “Fighting Money Launderers with Artificial Intelligence at HSBC.” *Google Cloud Blog FInancial Seervices* 1, no. 1 (November 30, 2023): 1–3. https://cloud.google.com/blog/topics/financial-services/how-hsbc-fights-money-launderers-with-artificial-intelligence.

Darem, Abdulbasit A., Asma A. Alhashmi, Tareq M. Alkhaldi, Abdullah M. Alashjaee, Sultan M. Alanazi, and Shouki A. Ebad. “Cyber Threats Classifications and Countermeasures in Banking and Financial Sector.” *IEEE Access* 11 (2023): 125138–58. https://doi.org/10.1109/ACCESS.2023.3327016.

Greenberg, Theodore S. *Politically Exposed Persons Preventive Measures For The Banking Sector*. Washington: The International Bank for Reconstruction and Development / The World Bank, 2010. DOI: 10.1596/978-0-8213-8249-3.

Hashimzai, Irshad Ahmed, and Mohammad Zameer Ahmadzai. “Navigating the Integration of Blockchain

Technology in Banking: Opportunities and Challenges." *International Journal Software Engineering and Computer Science (IJSECS)* 4, no. 2 (August 10, 2024): 665–79. https://doi.org/10.35870/ijsecs.v4i2.2656.

Israhadi, Evita Isretno. "Review of Digital Bank Law in Indonesia: Challenges in the Digital Era," n.d.

Jasa Keuangan, Otoritas. *Indonesia Banking Booklet 2023*. 10th ed. Jakarta, Indonesia: Otoritas Jasa Keuangan Department of Banking Licensing and Crisis Management, 2023.

Jorge, Guillermo. "Identification and Exchange of Information on Politically Exposed Persons in Central American Countries." Inter-American Development Bank, August 3, 2018. https://doi.org/10.18235/0010714.

Klimenko, Alla. "Digital Transformation in Banking and Financial Services." *Mad Devs*, September 24, 2024. https://maddevs.io/blog/digital-transformation-in-banking-and-financial-services/.

Kumar, Sumit. "Indonesia's Fintech Industry Is Ready to Rise." Indonesia, March 2023.

Laras, Arlina. "Top 7 Bank Digital Di Indonesia Kuartal I/2024: Seabank Teratas, Hibank Melesat," 2024. https://finansial.bisnis.com/read/20240525/90/1768141/top-7-bank-digital-di-indonesia-kuartal-i20.

Lazuardy, Moch Syahren, Maya Rachmawati, Tina Marlina, and Jaenudin Umar. "Legal Framework for Protecting Bank Customers against Personal Data Leakage in the Digital Era: A Study of Indonesian Regulations." *Indonesian Journal of Multidisciplinary Science* 3, no. 10 (July 25, 2024). https://doi.org/10.55324/ijoms.v3i10.907.

Lelono, Agus Joko, Mohamad Tohari, and Hono Sejati. "The Urgency of Legal Reform for the Legality of Digital Currency in Indonesia" 6, no. 4 (2024).

Mugarura, Norman. "Customer Due Diligence (CDD) Mandate and the Propensity of Its Application as a Global AML Paradigm." *Journal of Money Laundering Control* 17, no. 1 (January 7, 2014): 76–95. https://doi.org/10.1108/JMLC-07-2013-0024.

Munachi Ijeoma Ononiwu, Obianuju Clement Onwuzulike, and Kazeem Shitu. "Comparative Analysis of Customer Due Diligence and Compliance: Balancing Efficiency with Regulatory Requirements in the Banking Sectors of the United States and Nigeria." *World Journal of Advanced Research and Reviews* 23, no. 3 (September 30, 2024): 475–91. https://doi.org/10.30574/wjarr.2024.23.3.2707.

Mushtaq, Ahmad. "Compliance Challenges and Tech-Driven Solutions in Combating Financial Crime Within the Fintech Ecosystem." *Lovely Professional University* 4, no. 1 (May 2024): 62–80. https://doi.org/DOI:10.4018/979-8-3693-3633-5.ch005.

Negara Malaysia, Bank. "Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions (AML/CFT/CPF and TFS for FIs)." *Central Bank of Malaysia*, February 5, 2024, 1–175.

Partners, Assegaf Hamzah. "OJK Embraces Digital Bank with New Regulations." *Rajah & Tann Asia Lawyers Who Know Asia* 1, no. 1 (November 2021): 1–6. https://www.ahp.id/clientalert/AHPClientUpdate-4November2021.pdf.

Patience Okpeke Paul and Toluwalase Vanessa Iyelolu. "Anti-Money Laundering Compliance and Financial Inclusion: A Technical Analysis of Sub-Saharan Africa." *GSC Advanced Research and Reviews* 19, no. 3 (June 30, 2024): 336–43. https://doi.org/10.30574/gscarr.2024.19.3.0235.

Rithmaya, Chitra Laksmi, Herwin Ardianto, and Evi Sistiyarini. "GEN Z AND THE FUTURE OF BANKING: AN ANALYSIS OF DIGITAL BANKING ADOPTION." *Jurnal Manajemen Dan Kewirausahaan* 26, no. 1 (March 1, 2024): 64–78. https://doi.org/10.9744/jmk.26.1.64-78.

Rusdiana, Shelvi. "Rethinking Indonesian Anti-Money Laundering Laws in the Age of Online Gaming Economies." *NURANI: JURNAL KAJIAN SYARI'AH DAN MASYARAKAT* 24, no. 2 (October 23, 2024): 360–74. https://doi.org/10.1910 9/nurani.v24i2.24422.

Rusli, Ganda Raharja, and Anestia Hayubriandini Fermay. "Digital Financial Services Effort in Enforcing Anti-Money Laundering through Open Banking Optimization." *AML/CFT Journal The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 2 (June 1, 2024): 159–74. https://doi.org/10.59593/amlcft.2024.v2i2.158.

Sugianto, Fajar, and Joshua Evandeo Irawan. “Urgensi Menjadikan Hasil Analisis (HA)/Hasil Pemeriksaan (HP) PPATK Sebagai Alat Bukti Dalam Perkara TPPU Dan TPPT Di Indonesia.” *AML/CFT Journal The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 2 (June 1, 2024): 147–58. https://doi.org/10.59593/amlcft.2024.v2i2.153.

UNCTAD, ed. *Tackling Illicit Financial Flows for Sustainable Development in Africa*. Economic Development in Africa Report 2020. Geneva: United Nations, 2020.

Wimbah, Santoso. “Financial Services Authority to Improve Digitalization of Financial Sector.” *Cabinet Secretariat of The Republic of Indonesia* 1, no. 1 (2021): 1–2. https://setkab.go.id/en/financial-services-authority-to-improve-digitalization-of-financial-sector/.

Wiwoho, Jamal, Dona Budi Kharisma, and Dwi Tjahja K. Wardhono. “Financial Crime In Digital Payments.” *Journal of Central Banking Law and Institutions* 1, no. 1 (December 28, 2021): 47–70. https://doi.org/10.21098/jcli.v1i1.7.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. “Personal Data Protection Law in Digital Banking Governance in Indonesia.” *Studia Iuridica Lublinensia* 32, no. 1 (March 28, 2023): 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130.