Lex Publica
Jurnal Ilmu Hukum Asosiasi Pimpinan Perguruan Tinggi Hukum Indonesia
e-ISSN: 2579-8855
p-ISSN: 2354-9181
https://journal.appthi.org/index.php/lexpublica

Strengthening the Gatekeeper Function of Banks: The Role of KYC in Anti-Money Laundering Legal Framework

Efendi Lod Simanjuntak[1*], Gautam Kumar Jha[2]

[1]Universitas Borobudur, Jakarta, Indonesia
[2]Universitas Jawaharlal Nehru, New Delhi, India

**Corresponding author: efendi@uhb.ac.id*

Abstract. This study critically examines the role of Know Your Customer (KYC) compliance within Indonesia's anti-money laundering and counter-terrorism financing (AML/CFT) framework. Employing a normative juridical approach, the research analyzes key regulatory instruments, including Law Number 8 of 2010, POJK Number 12/POJK.01/2017, and the institutional role of PPATK, alongside relevant legal doctrines and international standards, particularly those of the Financial Action Task Force (FATF). The study addresses three core issues: the structuring of KYC obligations within Indonesia's legal framework, the implementation of KYC principles by financial institutions as part of risk management strategies, and the challenges encountered in practice. The findings demonstrate that KYC functions as a central legal and operational instrument, enabling customer identification, transaction monitoring, and reporting of suspicious activities, thereby reinforcing the banking sector's role as a gatekeeper in preventing financial crimes. However, its effectiveness is constrained by data quality issues, technological limitations, uneven institutional capacity, and increasingly sophisticated laundering techniques. The study concludes that strengthening regulatory enforcement, enhancing technological adoption (including RegTech and AI), and improving inter-agency coordination are essential to optimize KYC effectiveness.

Keywords: Laundering (AML/CFT), Banking Regulation, Indonesia, KYC Compliance, Risk Anti-Management.

Received: August 12, 2025 | Revised: November 3, 2025 | Accepted: December 15, 2025

Lex Publica
Vol. 12, No. 2, 2025, 448-472

DOI: https://doi.org/10.58829/lp.12.2.2025.320

Abstrak. *Studi ini secara kritis meneliti peran kepatuhan Know Your Customer (KYC) dalam kerangka anti pencucian uang dan pendanaan terorisme (AML/CFT) di Indonesia. Dengan menggunakan pendekatan yuridis normatif, penelitian ini menganalisis instrumen regulasi utama, termasuk Undang-Undang Nomor 8 Tahun 2010, POJK No. 12/POJK.01/2017, dan peran kelembagaan PPATK, bersama dengan doktrin hukum dan standar internasional yang relevan, khususnya standar Gugus Tugas Aksi Keuangan (FATF). Studi ini membahas tiga isu inti: penataan kewajiban KYC dalam kerangka hukum Indonesia, implementasi prinsip KYC oleh lembaga keuangan sebagai bagian dari strategi manajemen risiko, dan tantangan yang dihadapi dalam praktik. Temuan menunjukkan bahwa KYC berfungsi sebagai instrumen hukum dan operasional utama, yang memungkinkan identifikasi pelanggan, pemantauan transaksi, dan pelaporan aktivitas mencurigakan, sehingga memperkuat peran sektor perbankan sebagai penjaga gerbang dalam mencegah kejahatan keuangan. Namun, efektivitasnya dibatasi oleh masalah kualitas data, keterbatasan teknologi, kapasitas kelembagaan yang tidak merata, dan teknik pencucian uang yang semakin canggih. Studi ini menyimpulkan bahwa penguatan penegakan peraturan, peningkatan adopsi teknologi (termasuk RegTech dan AI), dan peningkatan koordinasi antar lembaga sangat penting untuk mengoptimalkan efektivitas KYC.*

Kata kunci: *Pencucian Uang (AML/CFT), Regulasi Perbankan, Indonesia, Kepatuhan KYC, Manajemen Risiko.*

1. Introduction

The rapid expansion of the global financial system has significantly contributed to economic growth, cross-border investment, and international trade. However, this development has also intensified the exposure of the financial sector, particularly the banking industry, to various forms of financial crime. Among these, money laundering remains one of the most serious and complex threats to the integrity of financial institutions and the stability of national and global economies.[1] Money laundering enables the concealment and legitimization of proceeds derived from illegal activities such as corruption, drug trafficking, terrorism financing, and organized crime, thereby undermining financial transparency and governance structures.[2]

Money laundering typically operates through the manipulation of banking systems, which are inherently designed to facilitate large-scale, rapid, and cross-border financial transactions. The process generally occurs in three stages: placement, layering, and integration, all of which often rely on banking channels to obscure the illicit origin of funds.[3] Consequently, banks function as the first line of defense in detecting and preventing such illegal financial flows.[4] The increasing sophistication of laundering techniques, supported by digital banking and financial technologies, has further complicated detection and enforcement efforts, creating new vulnerabilities within financial systems.[5]

In response to these challenges, international and national regulatory frameworks have been strengthened. The Financial Action Task Force (FATF), established in 1989, has developed global Anti-Money Laundering (AML) standards that require member states to implement robust preventive measures within their financial systems.[6] Indonesia has adopted these standards through Law

[1] Muhammad Saleem Korejo et al., "The concept of money laundering: a quest for legal definition," *Journal of Money Laundering Control* 24, no. 4 (2021): 728. See also, Michael Levi, and Peter Reuter, "Money laundering." *Crime and justice* 34, no. 1 (2006): 290.

[2] Peter Reuter, *Chasing dirty money: The fight against money laundering* (Washington: Peterson Institute, 2005), 33. See also, Georgy Rusanov, and Yury Pudovochkin, "Money laundering in the modern crime system," *Journal of money laundering control* 24, no. 4 (2021): 862.

[3] Michele Riccardi, and Peter Reuter, "The varieties of money laundering and the determinants of offender choices," *European Journal on Criminal Policy and Research* 30, no. 3 (2024): 336. See also, Reuter, *Chasing dirty money,* 35.

[4] Ting-Hsuan Chen, "Do you know your customer? Bank risk assessment based on machine learning," *Applied Soft Computing* 86 (2020): 105779.

[5] Chengzu Dong et al., "A blockchain-based self-sovereign identity system for KYC processes," In *Proceedings of the 6th ACM international symposium on blockchain and secure critical infrastructure*, (2024), 9.

[6] Financial Action Task Force (FATF), *Annual Report 2022–2023* (Paris: FATF/OECD, 2023), 34.

Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, which obligates financial institutions to detect, monitor, and report suspicious transactions to the Financial Transaction Reports and Analysis Centre (PPATK).[7] These legal frameworks position banks as critical actors in the implementation of AML policies.

A central mechanism in the AML regime is the Know Your Customer (KYC) principle. KYC requires banks to verify customer identities, understand the nature of their financial activities, and continuously monitor transactions to identify suspicious behavior.[8] Through this process, financial institutions are able to construct customer risk profiles that support early detection of anomalies and potential illicit financial activity.[9] Moreover, KYC is closely integrated with broader AML compliance systems and contributes significantly to regulatory enforcement and financial security.

Beyond its preventive function, KYC also plays a critical role in shaping financial institutions' risk management strategies. First, KYC enables risk identification and assessment by categorizing customers based on risk levels, including politically exposed persons (PEPs) and high-risk entities, while supporting fraud and default risk detection through data-driven analysis.[10] Second, KYC contributes to risk mitigation by ensuring compliance with AML and counter-terrorism financing regulations, thereby reducing legal, operational, and reputational risks for financial institutions.[11] Third, KYC enhances operational efficiency through digitalization, automation, and centralized data systems, which improve the accuracy and speed of customer verification and monitoring processes.[12]

However, despite its importance, the implementation of KYC in Indonesia remains inconsistent and faces persistent structural and operational challenges. In

[7] PPATK Regulation No. 9 of 2017 *on Procedures for Submission of Information on PPATK Examination Results to Investigators.*

[8] Nadine Kathrin Ostern, and Johannes Riedel, "Know-your-customer (KYC) requirements for initial coin offerings," *Business & Information Systems Engineering* 63, no. 5 (2021): 554.

[9] Constantin Cătălin Drăgan, and Mark Manulis, "KYChain: user-controlled KYC data sharing and certification," In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, (2020), 302. See also, Sasan Jafarnejad et al., "A risk-based AML framework: Finding associates through ultimate beneficial owners," In *2024 IEEE Symposium on Computational Intelligence for Financial Engineering and Economics (CIFEr)* (IEEE, 2024), 1.

[10] Budi Santoso et al., "Know Your Customer (KYC) Model: A Legal Reform Strategy to Prevent Abuse of Financial Services in Child Sexual Exploitation Transactions," *Journal of Law and Legal Reform* 6, no. 1 (2025): 243. See also, Chen, "Do you know your customer?" 105780.

[11] Dong et al., "A blockchain-based self-sovereign," 10.

[12] Cynthia Jayapal, and Harish Kumar RB, "Enhancing KYC Efficiency and Accuracy Through Session Recording and Document Auto-Capture," In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)* (New York: IEEE, 2023), 7.

practice, several issues continue to hinder its effectiveness, including inadequate technological infrastructure, limited institutional capacity, insufficient skilled human resources, and regulatory gaps that weaken enforcement consistency. Financial institutions are also sometimes driven by commercial interests that prioritize business expansion over strict compliance obligations, thereby reducing the effectiveness of Anti-Money Laundering (AML) controls. In addition, deficiencies in data quality, such as incomplete or inaccurate customer information caused by human error and system limitations, further undermine the reliability of KYC processes. Although electronic KYC (eKYC) has been introduced to improve efficiency, its impact on AML and counter-terrorism financing remains limited due to uneven implementation and moderate effectiveness in transaction monitoring.[13] Furthermore, the rapid development of financial technology and digital banking has introduced new risks, including anonymous transactions and cross-platform financial activities, which complicate traditional compliance mechanisms and increase exposure to financial crime risks.[14] Emerging technologies such as blockchain, artificial intelligence, and regulatory technology (RegTech) offer potential improvements in transparency, fraud detection, and compliance however, their effectiveness remains constrained by the absence of a comprehensive legal and governance framework in Indonesia.[15]

Despite extensive global literature on Know Your Customer (KYC) compliance, several important gaps remain, particularly in the context of developing financial systems such as Indonesia. Existing studies largely emphasize that KYC is essential for strengthening Anti-Money Laundering (AML) frameworks through customer identification, transaction monitoring, and risk

[13] Meiryani, "Prevention and control of money laundering crimes on know your customer principles application: empirical study of Indonesia banking sector," *Journal of Money Laundering Control* 27, no. 5 (2024): 875.

[14] Jonny Frank, and Laura Greenman, "Revisiting conduct risk management in the COVID-19 era with updated DOJ criteria," *Journal of Risk Management in Financial Institutions* 13, no. 4 (2020): 296.

[15] Douglas W. Arner et al., "FinTech, RegTech, and the reconceptualization of financial regulation," *Nw. J. Int'l L. & Bus.* 37 (2016): 372. See also, Md Abdul Hannan et al., "A systematic literature review of blockchain-based e-KYC systems," *Computing* (2023): 1; Bulut Karadag et al., "Blockchain-based KYC model for credit allocation in banking." *IEEE Access* 12 (2024): 80178; By Bhagvan Kommadi, "Blockchain An Elixir for Anti-Money Laundering?" *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (2019): 129; Pradnya Patil, and M. Sangeetha, "Blockchain-based decentralized KYC verification framework for banks," *Procedia Computer Science* 215 (2022): 531; N. Sumanti, and Madhavi Damle, "Transforming the KYC Process in Banking: Using Hyperautomation to Enhance Efficiency and Security," In *2025 International Conference on Technology Enabled Economic Changes (InTech)* (IEEE, 2025), 1219; Thomas Vinther Daugaard et al., "Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering." *Electronic Commerce Research and Applications* 65 (2024): 10138.

profiling.[16] KYC is also widely recognized as a core mechanism for enhancing financial institutions' risk management strategies by enabling fraud detection, regulatory compliance, and enhanced due diligence.[17]

However, most prior research tends to examine KYC in isolation as a compliance or technical requirement, rather than as an integrated strategic risk management instrument. While risk profiling and technological integration (AI, blockchain, and automation) are widely discussed, their combined impact on institutional risk governance structures remains underexplored.[18] Furthermore, existing studies often focus on developed financial markets, while evidence from emerging economies such as Indonesia remains fragmented and under-theorized, particularly regarding institutional capacity and regulatory enforcement gaps.[19]

Another critical gap lies in the limited empirical understanding of how KYC compliance directly influences the effectiveness of money laundering detection in banking operations. Although AI and machine learning are frequently proposed as solutions, their real-world effectiveness in improving AML outcomes in Indonesia remains inconsistent due to infrastructural and legal constraints.[20]

Given these challenges, there is a clear need to critically examine not only how KYC compliance is implemented within financial institutions, but also how it is structured within the broader legal and regulatory framework governing anti-

[16] Chen, "Do you know your customer?" 105781. See also, Meiryani, "Prevention and control of money laundering," 876.

[17] Dong et al., "A blockchain-based self-sovereign," 2. See also, Jafarnejad et al., "A risk-based AML framework," 2.

[18] Kristin Kamilla Kirss, and Fredrik Milani, "Using Blockchain Technology to Redesign Know-Your-Customer Processes Within the Banking Industry," In *International Conference on Business Process Management* (Cham: Springer International Publishing, 2020), 254. See also, José Lino Pereira et al., "Blockchain for Know Your Customer Process in Anti-money Laundering Compliance: A Review in Financial Services," In *Iberian Conference on Information Systems and Technologies* (Cham: Springer Nature Switzerland, 2025), 122; Jayapal, and Kumar RB, "Enhancing KYC Efficiency," 8.

[19] Longjie Lu, "Regulating ESG rating firms as the gatekeepers for sustainable finance," *Capital Markets Law Journal* 19, no. 2 (2024): 189. See also, Meiryani et al., "Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing," *Journal of Money Laundering Control* 26, no. 4 (2023): 895.

[20] Mohannad Alkhalili et al., "Investigation of applying machine learning for watch-list filtering in anti-money laundering," *iEEE Access* 9 (2021): 18484. See also, Fatema Tuz Johora et al., "AI advances: Enhancing banking security with fraud detection," In *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)* (IEEE, 2024), 291; Chen, "Do you know your customer?" 105783; Frank, and Greenman, "Revisiting conduct risk management," 297; Donkor Nawaah, and Rockson Mintah, "AI Applications for Anti-Money Laundering and Compliance in Financial Institutions," In *Foundations of Artificial Intelligence in Finance*, (Chapman and Hall/CRC, 2026), 149; Jose Ricardo Oliveira, and Adriano Galindo Leal, "Enhancing anti-money laundering protocols: Employing machine learning to minimise false positives and improve operational cost efficiency," In *Proceedings of the 2024 8th International Conference on Advances in Artificial Intelligence* (2024), 9.

money laundering. It is equally important to assess the effectiveness of its implementation in practice, particularly in addressing evolving financial crime risks. Accordingly, this study is guided by three main research questions:

1. How does the anti-money laundering legal framework in Indonesia regulate and structure KYC obligations for financial institutions?
2. How are KYC principles implemented by financial institutions as part of their risk management and anti-money laundering strategies?
3. What are the key challenges and limitations in the implementation of KYC compliance within Indonesia's AML/CFT framework?

By doing so, this study positions KYC not merely as a formal regulatory obligation, but as a dynamic instrument of risk governance within the financial system. It contributes to the broader discourse on financial regulation, institutional compliance, and the evolving challenges of combating money laundering in an increasingly complex and digitalized financial environment.

2. Research Methods

This study employs a normative legal research design aimed at examining the regulatory framework and practical implementation of Know Your Customer (KYC) compliance within Indonesia's AML/CFT regime. The research adopts a statutory and conceptual approach, focusing on the interpretation of legal norms, regulatory obligations, and their alignment with international standards, particularly those developed by the Financial Action Task Force (FATF).

The primary data consist of legal and regulatory instruments, including Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering, POJK No. 12/POJK.01/2017 on AML/CFT implementation in the financial services sector, and related regulatory guidelines issued by the Financial Services Authority (OJK) and the Indonesian Financial Transaction Reports and Analysis Center (PPATK). These are complemented by secondary sources, such as academic literature, policy reports, and prior empirical studies on KYC, AML/CFT compliance, and financial crime risk management.

Data collection is conducted through documentary and literature review, systematically identifying, classifying, and synthesizing relevant legal texts and scholarly works. The analysis applies a qualitative juridical method, emphasizing legal interpretation, comparative assessment with international standards, and critical evaluation of implementation challenges. This approach enables the study to assess both the normative strength of the regulatory framework and the practical limitations affecting KYC compliance in Indonesia.

3. Results and Discussion

3.1. Legal Construction of KYC Obligations within Indonesia's Anti-Money Laundering Framework

Money laundering, widely recognized as a transnational financial crime, has evolved alongside the development of modern financial systems and regulatory frameworks. The term itself "money laundering" was first popularized in the United States during the prosecution of Al Capone, where illicit proceeds from organized crime were disguised through legitimate business channels such as laundromats before being reintroduced into the formal economy.[21] This historical origin underscores a fundamental characteristic of money laundering: the transformation of illegal proceeds into assets that appear legitimate within the financial system.

Within the Indonesian legal context, money laundering is formally defined under Article 1(1) of Law Number 8 of 2010 as any act that fulfills the elements of a criminal offence in accordance with statutory provisions (Law No. 8 of 2010). Substantively, this law categorizes money laundering into three principal forms: active laundering (Article 3), passive laundering (Article 4), and offences involving the receipt or control of illicit proceeds (Article 5). These classifications reflect a comprehensive legal approach that not only targets perpetrators directly involved in disguising criminal assets but also those who knowingly benefit from such activities.

From a criminological perspective, money laundering is inherently linked to predicate offences such as corruption, narcotics trafficking, human trafficking, and other serious crimes. It is widely conceptualized as a "follow-up crime," meaning that its existence depends on prior unlawful activities that generate illicit financial gains. This interdependence provides a critical rationale for anti-money laundering (AML) regulation: by disrupting laundering mechanisms, the legal system simultaneously undermines the economic incentives driving organized crime.[22]

The operational dynamics of money laundering are typically explained through three sequential stages: placement, layering, and integration. Placement represents the initial entry of illicit funds into the financial system, often through techniques such as smurfing, cash deposits, or the purchase of financial instruments. This stage is particularly vulnerable to detection due to the proximity of funds to their criminal origin. The second stage, layering, involves complex transactions designed to obscure the audit trail, including cross-border transfers, the use of shell companies,

[21] Frank E. Bird et al., *Practical loss control leadership* (Loganville, GA: International Loss Control Institute, 1990), 21. See also, Tim Boekhout van Solinge, "Drugs and money: Managing the drug trade and crime-money in Europe," (2007): 699; Levi, and Reuter, "Money laundering," 292.

[22] William C. Gilmore, *Dirty money: The evolution of money laundering counter-measures*, Vol. 2. (Strasbourg: Council of Europe Publishing, 1999), 32. See also, Reuter, *Chasing dirty money,* 36.

and asset conversions.[23] Finally, integration reintroduces the "cleaned" funds into the legitimate economy, making detection significantly more difficult as the illicit origin becomes deeply concealed.

However, the traditional model of money laundering has been increasingly challenged by technological advancements. Emerging modalities such as cryptocurrency transactions, decentralized finance (DeFi), and the use of the dark web have introduced new layers of complexity that strain existing regulatory framewo rks.[24] These developments reinforce the need for adaptive legal and institutional mechanisms capable of responding to rapidly evolving financial crime patterns.

Against this backdrop, the Know Your Customer (KYC) principle emerges as a central pillar in the legal framework for preventing and eradicating money laundering. KYC refers to a set of mandatory procedures requiring financial institutions to identify, verify, and continuously monitor customer identities and transaction behaviors. Its conceptual origins can be traced to the recommendations of the Basel Committee on Banking Supervision (BCBS) in 1988, which were later institutionalized through the Financial Action Task Force (FATF) Forty Recommendations, now recognized as the global standard for AML compliance.[25]

In Indonesia, the KYC principle is operationalized through a structured regulatory framework that integrates Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and Simplified Due Diligence (SDD). CDD constitutes the baseline requirement, encompassing identity verification, beneficial ownership identification, and understanding the purpose of the business relationship. EDD applies stricter scrutiny to high-risk customers such as Politically Exposed Persons (PEPs) or clients from high-risk jurisdictions while SDD allows simplified procedures for low-risk customers, consistent with a risk-based approach. This tiered structure reflects a nuanced regulatory design aimed at balancing effectiveness and efficiency in AML implementation.[26]

---

[23] Effendi Lod Simanjuntak, *Penegakan Hukum Pencucian Uang Lintas Negara*, *Teori dan Praksis Penerapan MLA di ASEAN* (Yogyakarta: Arti Bumi Intaran, 2022), 42.

[24] Rainer Böhme et al., "Bitcoin: Economics, technology, and governance," *Journal of economic Perspectives* 29, no. 2 (2015): 221. See also, Financial Action Task Force (FATF), *The FATF Recommendations* (Paris: FATF/OECD, 2021), 23.

[25] Financial Action Task Force (FATF), *Guidance on Risk-Based Approach for the Banking Sector* (Paris: FATF/OECD, 2014), 43. See also, Basel Committee on Banking Supervision, *Customer Due Diligence for Banks. Basel*, Bank for International Settlements. No. (2001), 23.

[26] Bart Custers, "Risk profiling of money laundering and terrorism funding: Practical problems of current information strategies," In *Proceedings of the 9th International Conference on Enterprise Information Systems.* (Portugal: Funchal, 2007), 32. See also, Ainul Huda Jamil et al., "Money laundering risk judgement by compliance officers at financial institutions in Malaysia: the effects of customer risk determinants and regulatory enforcement," *Journal of Money Laundering Control* 26, no.

Indonesia's legal framework for AML is notably comprehensive and multi-layered, consisting of statutory provisions, regulatory instruments, and institutional mechanisms. Law Number 8 of 2010 serves as the cornerstone of this framework, introducing significant innovations such as the expansion of predicate offences, the strengthening of institutional authority, and the adoption of a reversed burden of proof mechanism.[27] Importantly, the law designates banks as key reporting entities, imposing obligations to submit Suspicious Transaction Reports (STR) and Cash Transaction Reports (CTR) to the Financial Transaction Reports and Analysis Centre (PPATK). Non-compliance with these obligations may result in both administrative and criminal sanctions.

A critical feature of this legal framework is the "safe harbour" provision under Article 25, which protects reporting entities acting in good faith from civil and criminal liability. This provision is essential in encouraging proactive reporting and enhancing the effectiveness of financial intelligence systems. Complementing the statutory framework, OJK Regulation No. 12/POJK.01/2017 provides detailed technical guidance on AML/CFT implementation, including KYC procedures, transaction monitoring, and institutional governance. The regulation adopts a risk-based approach, aligning Indonesia's AML practices with international standards while allowing flexibility in addressing varying risk profiles.

Institutionally, the central role of PPATK as Indonesia's Financial Intelligence Unit (FIU) further strengthens the legal framework. PPATK functions as the hub for receiving, analyzing, and disseminating financial transaction reports, thereby facilitating coordination between financial institutions and law enforcement agencies. Empirical data indicate that more than 78% of suspicious transaction reports originate from the banking sector, highlighting the strategic importance of banks as the primary gatekeepers in the AML ecosystem.[28] In this sense, banks act as the "first line of defense," where KYC mechanisms serve as the initial filter against illicit financial flows.

Beyond compliance, KYC plays a transformative role in shaping financial institutions' risk management strategies. By enabling comprehensive customer profiling and continuous transaction monitoring, KYC facilitates early identification of high-risk clients and suspicious activities.[29] This function is increasingly enhanced by the integration of advanced technologies such as artificial

3 (2023): 537; Giovanni Scarcella, "Qui tam and the bank secrecy act: a Public-Private enforcement model to improve anti-Money laundering efforts," *Fordham L. Rev.* 90 (2021): 1360.

[27] Erma Denniagi, "Analisis Ke-Ekonomian Pemidanaan Tindak Pidana Pencucian Uang Dalam Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang," *Lex Renaissance* 6, no. 2 (2021): 247.

[28] Meiryani et al., "Effectiveness of regulatory technology," 896.

[29] Drăgan, and Manulis, "KYChain: user-controlled KYC," 303. See also, Jafarnejad et al., "A risk-based AML framework," 4.

intelligence and machine learning, which allow for real-time detection of anomalies and predictive risk assessment.[30]

Table 1. Key AML/CFT Regulations in Indonesia

Regulation	Key Provisions	Bank Obligations
Law No. 8/2010	Prevention & eradication of TPPU; definitions, criminal provisions, PPATK authority	Reporting of STR & CTR; KYC implementation
POJK No. 12/2017	AML/CFT program in financial services; CDD, EDD, monitoring	Customer verification; periodic reports to OJK & PPATK
GR No. 43/2015	Wealth reporting; corruption-based TPPU	Wealth reports of official customers
PPATK Reg. No. 9/2017	Reporting procedures; goAML system	Electronic reporting via goAML
POJK No. 39/2019	Integrated anti-fraud strategy with AML/CFT	Fraud detection system & AML integration

Moreover, KYC contributes to risk mitigation by ensuring adherence to regulatory requirements, thereby reducing exposure to legal penalties and reputational damage.[31] The application of Enhanced Due Diligence further strengthens this function by incorporating complex risk indicators, including beneficial ownership structures and geopolitical risks, into institutional decision-making processes.[32] At the same time, technological innovations such as blockchain-based identity systems and centralized data repositories have improved operational efficiency, reduced duplication, and enhanced data accuracy.[33]

3.2. KYC Implementation as an Integral Part of Risk Management and AML Strategies in Financial Institutions

The implementation of Know Your Customer (KYC) principles within financial institutions represents a comprehensive and integrated framework that directly answers how institutions operationalize risk management and anti-money laundering (AML) strategies in practice. Rather than functioning as a purely administrative requirement, KYC is embedded across the entire lifecycle of the

[30] Chen, "Do you know your customer?" 105784. See also, Jayapal, and Kumar RB, "Enhancing KYC Efficiency," 9.

[31] Perizat Buzaubayeva et al., "Enhancing financial performance and risk management in Kazakhstan's banking sector," *Banks and Bank Systems* 19, no. 1 (2024): 158. See also, Dong et al., "A blockchain-based self-sovereign," 4.

[32] Jafarnejad et al., "A risk-based AML framework," 4.

[33] T. R. Lekhaa, and N. Ramya Devi, "Streamlining KYC Processes for Banks with Centralized Information Repository Using Design Thinking," In *International Conference on Big Data Innovation for Sustainable Cognitive Computing* (Cham: Springer Nature Switzerland, 2023), 126. See also, Pereira et al., "Blockchain for Know Your Customer," 123.

customer relationship, combining customer due diligence (CDD, SDD, EDD), transaction monitoring, reporting obligations for Suspicious Transaction Report and Currency Transaction Report (STR/CTR), and institutional governance into a unified risk-based system.

At the foundational level, the legal obligations of banks in applying KYC principles are extensive and cover all aspects of their interaction with customers. These obligations can be grouped into several core categories, beginning with customer identification and verification. Every bank is required to identify and verify the identity of prospective customers before establishing any business relationship or providing financial services. This includes verifying official identification documents, confirming residential addresses, and identifying the beneficial owner, particularly when the customer is a legal entity or acting on behalf of another party.[34] For corporate customers, this obligation extends further to include verification of articles of incorporation, ownership structures, identification of controlling parties, and understanding the nature of the business. The prohibition against fictitious or anonymous accounts reflects a preventive legal design aimed at eliminating opacity at the entry point of the financial system.

This identification process forms the core of Customer Due Diligence (CDD), which operates within a broader risk-based approach. Financial institutions classify customers based on their risk profiles and apply differentiated levels of scrutiny. Simplified Due Diligence (SDD) is applied to low-risk customers, allowing streamlined procedures, while Enhanced Due Diligence (EDD) is imposed on high-risk categories, such as politically exposed persons (PEPs), clients from high-risk jurisdictions, or entities with complex ownership structures. EDD requires deeper investigation, including analysis of beneficial ownership, source of funds, and adverse media exposure.[35] Through this tiered structure, KYC becomes directly integrated into risk management by ensuring that regulatory attention and resources are allocated proportionally to the level of risk.

Importantly, KYC obligations are not limited to initial onboarding but extend into ongoing due diligence. Banks are required to continuously update customer data and reassess risk profiles, particularly when there are significant changes in customer information. This dynamic approach ensures that risk assessment remains current and responsive to evolving customer behavior, reinforcing the proactive nature of modern risk management systems.

A central operational dimension of KYC implementation is transaction monitoring. Banks must continuously monitor all customer transactions to detect activities that are inconsistent with the customer's profile, characteristics, or established transaction patterns. This monitoring is conducted by IT-based systems

[34] Ostern, and Riedel, "Know-your-customer (KYC)," 556.
[35] Jafarnejad et al., "A risk-based AML framework," 6.

that generate alerts when suspicious patterns are detected. In practice, this includes identifying transactions linked to high-risk jurisdictions, those lacking clear economic purpose, or those involving individuals or entities listed on national or international sanctions or terrorism watchlists. These monitoring systems are integrated with screening databases and blocklists, enabling real-time detection and escalation of potential risks.

Technological advancement significantly enhances this function. The use of artificial intelligence and big data analytics allows financial institutions to process vast volumes of transaction data and identify complex patterns indicative of money laundering. AI-based AML systems can analyze millions of transactions simultaneously, uncovering hidden relationships and anomalies that would be difficult to detect through manual processes.[36] This integration of technology not only improves detection accuracy but also strengthens the overall risk management capacity of financial institutions, enabling them to respond more effectively to emerging threats.[37]

Closely linked to transaction monitoring is the obligation to report suspicious and large-value transactions. Banks are required to submit Suspicious Transaction Reports (STR/LTKM) and Cash Transaction Reports (CTR/LTKT) to the Financial Transaction Reports and Analysis Center (PPATK). STRs must be filed within three business days after suspicion arises, while CTRs are mandatory for cash transactions exceeding IDR 500 million. Reporting is conducted electronically using the goAML system developed by UNODC and adapted for Indonesia. This system ensures efficiency, standardization, and traceability in financial intelligence reporting.

The reporting obligation is reinforced by strict confidentiality requirements, particularly the anti-tipping off provision, which prohibits banks from informing customers that a report has been filed. This ensures that investigations are not compromised and highlights the dual responsibility of financial institutions: maintaining customer relationships while simultaneously fulfilling legal obligations to the state.

Beyond operational procedures, the implementation of KYC principles requires robust institutional structures. Banks must establish dedicated compliance

[36] Ramandeep Kaur Chhina, "Managing money laundering risks in commercial letters of credit: Are banks in danger of non-compliance? A case study of the United Kingdom," *Journal of Money Laundering Control* 19, no. 2 (2016): 159. See also, Howard Chitimira, and Sharon Munedzi, "Historical aspects of customer due diligence and related anti-money laundering measures in South Africa," *Journal of Money Laundering Control* 26, no. 7 (2023): 141; Mahima Raj et al., "The use of artificial intelligence in anti-money laundering (AML)." In *2024 3rd International conference on sentiment analysis and deep learning (ICSADL)* (New York: IEEE, 2024), 272.

[37] Jafarnejad et al., "A risk-based AML framework," 7. See also, Oliveira, and Leal, "Enhancing anti-money laundering," 10.

units or appoint AML/CFT compliance officers who report directly to the board of directors. These units are responsible for ensuring that all policies, procedures, and systems comply with regulatory requirements and are effectively implemented across all business lines. In addition, banks are required to conduct regular AML/CFT training programs for employees, particularly frontline staff and compliance officers. These programs cover regulatory frameworks, techniques for identifying suspicious transactions, and internal reporting procedures, thereby strengthening institutional capacity and awareness.[38]

The integration of these elements CDD/EDD/SDD, transaction monitoring, reporting, and governance demonstrates how KYC functions as a comprehensive risk management system. It enables financial institutions to identify, assess, and mitigate risks associated with financial crimes while ensuring compliance with regulatory frameworks. KYC data serves as a critical input for customer risk profiling, allowing institutions to detect high-risk clients, monitor behavioral patterns, and anticipate potential threats.[39] This proactive approach fosters a risk-aware organizational culture, where compliance is embedded into daily operations rather than treated as a reactive obligation.[40]

Within the broader financial system, banks play a strategic "gatekeeper" role. As the primary entry point for funds into the formal economy, banks serve as the first line of defense against money laundering. All financial flows must pass through the banking system, and it is at this stage that KYC procedures filter and screen transactions. If banks fail to perform this function effectively, illicit funds can easily enter the financial system and become significantly more difficult to trace and recover.[41]

Furthermore, banks act as active partners in law enforcement. When authorities identify indications of money laundering, banks are required to cooperate by providing transaction records, blocking accounts upon request, and supporting asset seizure and confiscation processes. The obligation to retain transaction data for extended periods typically five to ten years ensures the availability of reliable evidence for investigations and prosecutions. This

[38] Nadia Pocher et al., "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," *Electronic Markets* 33, no. 1 (2023): 37.

[39] Metouole Mwinbe Yves Ghislain Somda et al., "Implementation of Robotic Process Automation To Decrease the Time Requires For KYC Onboarding Process," In *2023 6th International Conference on Artificial Intelligence and Big Data (ICAIBD)* (New York: IEEE, 2023), 345. See also, Chen, "Do you know your customer?" 105787.

[40] Kosmas Kaprinis, "Internal compliance, risk management, and their impact on culture in financial firms," In *Corporate Governance and Culture in Financial Institutions* (Cheltenham: Edward Elgar Publishing, 2025), 266.

[41] Marco Cappai, and Giuseppe Colangelo, "Taming digital gatekeepers: the 'more regulatory approach'to antitrust law," *Computer Law & Security Review* 41 (2021): 1559.

collaborative dimension highlights how KYC implementation extends beyond internal compliance to support broader legal and enforcement frameworks.

The legal consequences of failing to implement KYC and AML obligations are significant and reinforce their importance within risk management strategies. Regulatory authorities, such as the Financial Services Authority (OJK), have the power to impose a range of administrative sanctions, including warnings, fines, restrictions on business activities, suspension, and license revocation. These sanctions are applied proportionally based on the severity of the violation. In addition, criminal liability may arise where institutions or their management are found to have facilitated money laundering, whether intentionally or through negligence. Corporate entities may face substantial fines, while individuals may be subject to severe imprisonment penalties.[42]

In this context, KYC compliance not only mitigates financial crime risks but also protects institutions from legal, financial, and reputational consequences. It enhances operational efficiency through the use of digital technologies, such as automated verification systems, centralized data repositories, and blockchain-based solutions, which streamline processes and improve data accuracy.[43] At the same time, it strengthens the effectiveness of AML frameworks by enabling real-time detection, reporting, and response to suspicious activities.

In sum, the practical implementation of KYC principles in financial institutions reflects a holistic integration of regulatory compliance and risk management. Through structured due diligence (CDD, SDD, EDD), continuous transaction monitoring, systematic reporting (STR/CTR), and strong institutional governance, KYC operates as a dynamic and adaptive system. It not only fulfills legal requirements but also enhances the capacity of financial institutions to prevent, detect, and respond to financial crimes. By embedding KYC into their operational and strategic frameworks, financial institutions effectively position themselves as both regulators of risk and guardians of financial system integrity.

Table 2. Bank Obligations Under the KYC Principle

Obligation Aspect	Legal Basis	Consequences of Violation
Customer identification & verification	POJK 12/2017 Art. 14–25	Administrative sanctions; transaction ban
Ongoing transaction monitoring	POJK 12/2017; Law No. 8/2010 Art. 18	Admin sanctions; criminal liability for facilitated TPPU
Reporting STR & CTR to PPATK	Law No. 8/2010 Art. 23–25	Imprisonment & fines; OJK administrative sanctions

[42] Yoga Sugama Ali Fhatnur, "Dynamics and Strategies of Law Enforcement of Money Laundering Offences in Indonesia: Dinamika dan Strategi Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia," *Indonesian Journal of Law and Economics Review* 19, no. 2 (2024): 21070.

[43] Jayapal, and Kumar RB, "Enhancing KYC Efficiency," 10. See also, Kirss, and Milani, "Using Blockchain Technology," 255; Lekhaa, and Devi, "Streamlining KYC Processes," 127.

AML/CFT training program	POJK 12/2017 Art. 47–52	Written warning; restriction of business activities
Establishment of the compliance unit	POJK 12/2017; OJK Circular	Warning: license restriction
Anti-tipping off compliance	Law No. 8/2010 Art. 25	Imprisonment up to 5 years + fine up to IDR 1 billion

3.3. Challenges and Limitations in the Implementation of KYC Compliance within Indonesia's AML/CFT Framework

Although Indonesia's AML/CFT regulatory framework is relatively comprehensive, the practical implementation of the Know Your Customer (KYC) principle continues to encounter significant and persistent challenges. These limitations arise not only from technical and infrastructural constraints but also from institutional tensions, evolving financial crime patterns, and broader policy trade-offs. Despite regulatory advancements, issues related to data quality, technological disparities among financial institutions, and the continuous evolution of laundering techniques remain substantial obstacles.[44] At the same time, the necessity to balance strict compliance requirements with financial inclusion objectives creates an additional layer of regulatory complexity.

At a normative level, banks' legal obligations in implementing KYC are broad and comprehensive, covering the entire customer relationship lifecycle, including identification, verification, ongoing due diligence, transaction monitoring, reporting, and the establishment of internal compliance systems.[45] Banks must verify customer identities using official documents, confirm residential addresses, and identify beneficial owners, particularly for corporate clients. For legal entities, this also involves examining incorporation documents, ownership structures, controlling parties, and the nature of business activities. The prohibition of anonymous or fictitious accounts, combined with continuous data updates through ongoing due diligence, reflects the preventive orientation of KYC frameworks.

However, the effectiveness of these obligations is highly dependent on the quality of customer data. In Indonesia, persistent issues such as incomplete, inaccurate, or outdated data significantly weaken customer risk profiling and reduce the reliability of KYC systems. This undermines the detection of suspicious activities at an early stage. Significant disparities exist between large commercial banks and smaller institutions, particularly Rural Banks (BPR) and regional banks, which often lack the sophisticated infrastructure required to meet regulatory standards.[46]

[44] Meiryani et al., "Effectiveness of regulatory technology," 897.

[45] Ostern, and Riedel, "Know-your-customer (KYC)," 557.

[46] Kanon Mommsen Wongkar, "Implementation of KYC Principles for Indonesian Payment Services Provider," *Journal of Accounting, Business and Management (JABM)* 32, no. 1 (2024): 209.

The reporting obligation to the Indonesian Financial Transaction Reports and Analysis Center (PPATK) further illustrates operational challenges. Banks must submit Suspicious Transaction Reports (STR/LTKM) within three working days of identifying suspicious transactions and Cash Transaction Reports (CTR/LTKT) for transactions exceeding IDR 500 million. Reporting is conducted electronically through the goAML system, and is subject to strict confidentiality requirements under the anti–tipping-off principle. While these mechanisms are designed to enhance financial intelligence, their effectiveness depends on the capacity of bank personnel to accurately identify suspicious patterns. In practice, limitations in training and expertise particularly among frontline staff can hinder timely and accurate reporting.[47]

Institutionally, banks are required to establish compliance units and appoint AML/CFT compliance officers responsible for overseeing adherence to regulatory standards. However, internal resistance remains a recurring challenge. There is often a structural tension between business units focused on growth and profitability and compliance units tasked with enforcing KYC procedures. From a business perspective, KYC requirements may be perceived as burdensome, potentially slowing customer onboarding and reducing competitiveness. This tension can result in minimalistic compliance practices, where KYC is implemented as a formal obligation rather than a strategic risk management tool.

The rapid evolution of money laundering techniques further complicates KYC implementation. Perpetrators continuously adapt to regulatory controls, exploiting gaps in detection systems and leveraging emerging financial technologies. The rise of cryptocurrencies, decentralized finance (DeFi), and blockchain-based transactions introduces new challenges, as these systems often enable pseudonymous transactions and complex ownership structures that are difficult to trace.[48] While advanced technologies such as artificial intelligence and machine learning offer potential solutions for enhancing detection capabilities, their implementation remains uneven. Challenges related to integration, scalability, and regulatory uncertainty particularly regarding AI governance limit their effectiveness.

At the same time, the integration of technology into KYC processes presents both opportunities and constraints. Digital KYC systems, blockchain-based identity verification, and AI-driven monitoring tools have demonstrated the potential to improve efficiency, reduce operational costs, and enhance accuracy.[49]

---

[47] Pocher et al., "Detecting anomalous cryptocurrency transactions," 38.

[48] Fitri Komariyah, "Penerapan Prinsip Know Your Customer (KYC) dalam Mencegah Tindak Pidana Pencucian Uang," *Jurnal Manajemen dan Administrasi Bisnis (JUMASIS)* 1, no. 2 (2025): 59.

[49] Aryan Ghatge et al., "Automation in the KYC Process," In *International Conference on ICT for Sustainable Development* (Cham: Springer Nature Switzerland, 2025), 421. See also, Jayapal, and Kumar RB, "Enhancing KYC Efficiency," 11; Kirss, and Milani, "Using Blockchain Technology," 259.

These technologies enable faster onboarding, automated document verification, and real-time transaction analysis. However, their adoption requires substantial investment and technical expertise, which may not be accessible to all financial institutions. Furthermore, integration barriers and system compatibility issues remain significant challenges.[50]

Another critical dimension of KYC implementation is its impact on financial inclusion. Overly stringent KYC requirements may inadvertently exclude individuals who lack formal identification or documentation, particularly in rural or underserved areas. This creates a paradox within regulatory policy: while strict KYC measures are essential for preventing financial crimes, they may also limit access to formal financial services, thereby pushing vulnerable populations toward informal and less regulated financial systems (World Bank, 2021; Beck et al., 2007). Achieving a balance between compliance and inclusivity remains a complex and ongoing policy challenge.

The cross-border nature of modern money laundering further amplifies these challenges. Illicit financial flows often involve multiple jurisdictions, exploiting regulatory inconsistencies and banking secrecy laws. Indonesia has responded by actively participating in international cooperation frameworks, including the Asia Pacific Group on Money Laundering (APG) and the Egmont Group of Financial Intelligence Units. Through these mechanisms, PPATK can exchange financial intelligence with more than 160 jurisdictions and has established bilateral agreements with over 80 Financial Intelligence Units.[51] While these collaborations enhance the capacity to trace cross-border transactions, they also impose additional compliance requirements on domestic institutions, necessitating alignment with international standards. Moreover, the lack of global standardization in KYC processes creates additional challenges for institutions operating across borders, as they must navigate differing compliance requirements.[52]

From a systemic perspective, banks play a critical gatekeeper role within the AML/CFT architecture. As the primary entry point for funds into the formal financial system, banks function as the first line of defense against money laundering. Empirical evidence indicates that more than 78% of suspicious transaction reports submitted to PPATK originate from the banking sector, underscoring its central role in financial intelligence. However, this role also highlights systemic vulnerabilities: failures in KYC implementation can allow illicit

[50] Mohammad Haroun Sharairi, "Mapping Conceptual Frameworks for Real Time Fraud Risk Management in Digital Microfinance," *Enterprise Development and Microfinance* 35, no. 1 (2025): 304.

[51] Olha Bondarenko et al., "Mechanisms for interaction of law enforcement agencies in the field of countering money laundering," *Journal of Money Laundering Control* 27, no. 1 (2024): 42. See also, Simanjuntak, *Penegakan Hukum Pencucian Uang*, 44.

[52] Hans-Joachim Von Haenisch, and Thomas Egner, "Know your customer: Unravelling the challenges," *Journal of Payments Strategy & Systems* 18, no. 1 (2024): 33.

funds to enter the financial system, making them significantly more difficult to trace and recover.[53]

Table 3. Key Components of an Effective KYC Process in Anti-Money Laundering (AML) Frameworks

Component	Description	Reference
Customer Identification	Verifying identities to ensure legitimacy	(Zentoni et al., 2025; Doughty, 2005; Wood, 2012)[54]
Continuous Monitoring	Detecting suspicious activities through ongoing surveillance	(Zentoni et al., 2025; Doughty, 2005; Raj et al., 2024)[55]
Use of Technology	Leveraging blockchain, AI, and automated systems for efficiency and security	(Pereira et al., 2026; Hannan et al., 2023; Vinoth Kumar et al., 2024)[56]
Risk Assessment	Profiling customers and assessing risks based on various indicators	(Jafarnejad et al., 2024; Tuba & Van Der Westhuizen, 2014)[57]
Privacy and Security	Protecting customer data while ensuring compliance	(Hannan et al., 2023; Xiong et al., 2025)[58]
Collaboration & Standards	Promoting global standardization and cooperation with authorities	(Zentoni et al., 2025; Doughty, 2005; Hannan et al., 2023)[59]

KYC compliance plays a central role in shaping financial institutions' risk management strategies by enabling systematic customer risk profiling, identification of high-risk individuals such as politically exposed persons (PEPs), and continuous monitoring of transaction behavior.[60] Through mechanisms such as enhanced due diligence (EDD), banks are able to assess complex risk dimensions, including beneficial ownership structures, adverse exposure, and

[53] Cappai, and Colangelo, "Taming digital gatekeepers," 1560.

[54] Caroline Doughty, "Know your customer: Automation is key to comply with legislation," *Business information review* 22, no. 4 (2005): 249. See also, Jenny Wood, *Global business practises* (EuroAsia Semiconductor, 2012), 43.

[55] Doughty, "Know your customer," 250. See also, Raj et al., "The use of artificial intelligence," 274.

[56] Hannan et al., "A systematic literature review," 2. See also, Pereira et al., "Blockchain for Know Your Customer," 125; C. Vinoth Kumar et al., "Ethereum blockchain framework enabling banks to know their customers," *IEEE Access* 12 (2024): 101358.

[57] Maphuti Tuba, and Chinelle Van der Westhuizen, "An analysis of the 'know your customer'policy as an effective tool to combat money laundering: is it about who or what to know that counts?" *International Journal of Public Law and Policy* 4, no. 1 (2014): 56. See also, Jafarnejad et al., "A risk-based AML framework," 8.

[58] Xihan Xiong et al., "REGKYC: Supporting privacy and compliance enforcement for KYC in blockchains," In *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE, 2025), 34. See also, Hannan et al., "A systematic literature review," 3.

[59] Doughty, "Know your customer," 252. See also, Hannan et al., "A systematic literature review," 4.

[60] Drăgan, and Manulis, "KYChain: user-controlled KYC," 305. See also, Jafarnejad et al., "A risk-based AML framework," 9.

jurisdictional risks. The integration of KYC within broader AML frameworks further strengthens institutional capacity to detect and respond to financial crimes in real time, particularly when supported by data-driven monitoring systems.[61] At a strategic level, this transforms KYC from a procedural requirement into a proactive risk management instrument. However, the effectiveness of these strategies remains highly contingent upon data quality, technological capability, and the organizational commitment to compliance.

At the same time, violations of AML/CFT obligations carry significant legal consequences. Regulatory authorities, particularly the Financial Services Authority (OJK), possess broad enforcement powers, including the imposition of administrative sanctions ranging from written warnings and financial penalties to restrictions on business activities and license revocation. In more serious cases, criminal liability may be imposed on both institutions and their management. Under Indonesian law, corporate entities may face fines of up to IDR 100 billion, while individuals can be subject to imprisonment of up to 20 years for involvement in money laundering activities.[62] Despite the severity of these sanctions, their deterrent effect depends on supervisory effectiveness and consistent regulatory enforcement.

In this context, while technological innovations such as artificial intelligence, blockchain, and centralized data systems offer significant potential to enhance KYC efficiency and accuracy, their implementation remains uneven. Overall, the effectiveness of KYC compliance in Indonesia is shaped by the interaction between regulatory strength, institutional capacity, and the evolving complexity of financial crime, requiring continuous adaptation and a more integrated risk-based compliance culture.

4. Conclussion

Indonesia has established a comprehensive legal framework for preventing and eradicating money laundering, primarily anchored in Law No. 8 of 2010, complemented by POJK No. 12/POJK.01/2017 and the institutional role of PPATK as the national financial intelligence unit. This framework aligns with FATF standards and positions the banking sector as a central actor in the anti-money laundering (AML/CFT) regime. Banks are required to implement the KYC principle through customer due diligence (CDD/EDD), continuous transaction monitoring, reporting of suspicious and cash transactions (STR/CTR) to PPATK, AML/CFT training programs, and the establishment of independent compliance

[61] Dong et al., "A blockchain-based self-sovereign," 6. See also, Pereira et al., "Blockchain for Know Your Customer," 128.

[62] Fhatnur, "Dynamics and Strategies of Law," 21071.

units. These obligations are comprehensive and binding across all operational levels.

The banking sector functions as a strategic gatekeeper, serving as the first line of defence and contributing the majority of financial intelligence reports, thereby supporting law enforcement efforts. However, despite this robust normative framework, the practical implementation of KYC remains constrained by several challenges, including data quality issues, technological disparities, particularly among smaller banks, internal organizational resistance, and the rapid evolution of money laundering techniques. Additionally, regulatory efforts must carefully balance strict compliance requirements with financial inclusion objectives. To enhance effectiveness, strengthening international cooperation and accelerating the adoption of RegTech and AI-based systems are essential. Policy recommendations include improving risk-based supervision by OJK, enhancing PPATK's analytical capacity and inter-agency coordination, updating legal frameworks to address emerging digital risks, and promoting further empirical research on KYC effectiveness within both national and comparative regional contexts.

References

Alkhalili, Mohannad, Mahmoud H. Qutqut, and Fadi Almasalha. "Investigation of applying machine learning for watch-list filtering in anti-money laundering." *iEEE Access* 9 (2021): 18481-18496.

Arner, Douglas W., Janos Barberis, and Ross P. Buckey. "FinTech, RegTech, and the reconceptualization of financial regulation." *Nw. J. Int'l L. & Bus.* 37 (2016): 371.

Basel Committee on Banking Supervision (2001), *Customer Due Diligence for Banks. Basel*, Bank for International Settlements.

Bird, Frank E., George L. Germain, and M. Douglas Clark. *Practical loss control leadership*. Loganville, GA: International Loss Control Institute, 1990.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, technology, and governance." *Journal of economic Perspectives* 29, no. 2 (2015): 213-238.

Bondarenko, Olha, Maryna Utkina, Oleg Reznik, and Mykhailo Dumchikov. "Mechanisms for interaction of law enforcement agencies in the field of countering money laundering." *Journal of Money Laundering Control* 27, no. 1 (2024): 34-50.

Buzaubayeva, Perizat, Aigul Orazbayeva, Gulzhan Alina, Zamzagul Baimagambetova, and Gulzhihan Kenges. "Enhancing financial performance and risk management in Kazakhstan's banking sector." *Banks and Bank Systems* 19, no. 1 (2024): 157.

Cappai, Marco, and Giuseppe Colangelo. "Taming digital gatekeepers: the 'more regulatory approach'to antitrust law." *Computer Law & Security Review* 41 (2021): 105559.

Chen, Ting-Hsuan. "Do you know your customer? Bank risk assessment based on machine learning." *Applied Soft Computing* 86 (2020): 105779.

Chhina, Ramandeep Kaur. "Managing money laundering risks in commercial letters of credit: Are banks in danger of non-compliance? A case study of the United Kingdom." *Journal of Money Laundering Control* 19, no. 2 (2016): 158-168.

Chitimira, Howard, and Sharon Munedzi. "Historical aspects of customer due diligence and related anti-money laundering measures in South Africa." *Journal of Money Laundering Control* 26, no. 7 (2023): 138-154.

Custers, Bart. "Risk profiling of money laundering and terrorism funding: Practical problems of current information strategies." In *Proceedings of the 9th International Conference on Enterprise Information Systems. Funchal, Portugal.* 2007.

Daugaard, Thomas Vinther, Jakob Bisgaard Jensen, Robert J. Kauffman, and Kwansoo Kim. "Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering." *Electronic Commerce Research and Applications* 65 (2024): 101386.

Denniagi, Erma. "Analisis Ke-Ekonomian Pemidanaan Tindak Pidana Pencucian Uang Dalam Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang." *Lex Renaissance* 6, no. 2 (2021): 246-264.

Dong, Chengzu, Aiting Yao, Zhiyu Xu, Meiqu Lu, Frank Jiang, Shiping Chen, and Xiao Liu. "A blockchain-based self-sovereign identity system for KYC processes." In *Proceedings of the 6th ACM international symposium on blockchain and secure critical infrastructure*, pp. 1-11. 2024.

Doughty, Caroline. "Know your customer: Automation is key to comply with legislation." *Business information review* 22, no. 4 (2005): 248-252.

Drăgan, Constantin Cătălin, and Mark Manulis. "KYChain: user-controlled KYC data sharing and certification." In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 301-307. 2020.

Fhatnur, Yoga Sugama Ali. "Dynamics and Strategies of Law Enforcement of Money Laundering Offences in Indonesia: Dinamika dan Strategi Penegakan Hukum Tindak Pidana Pencucian Uang di Indonesia." *Indonesian Journal of Law and Economics Review* 19, no. 2 (2024): 10-21070.

Financial Action Task Force (FATF). *Annual Report 2022–202*3. Paris: FATF/OECD, (2023).

Financial Action Task Force (FATF). *Guidance on Risk-Based Approach for the Banking Sector.* Paris: FATF/OECD, (2014).

Financial Action Task Force (FATF). *The FATF Recommendations*. Paris: FATF/OECD, (2021).

Financial Services Authority (OJK). *Indonesian Banking Development Roadmap 2020–2025*. Jakarta: OJK, 2020.

Financial Services Authority (OJK). *Indonesian Banking Statistics, December 2022*. Jakarta: OJK, (2023).

Financial Transaction Reports and Analysis Centre (PPATK). (2023). *Annual Report* 2022. Jakarta: PPATK.

Frank, Jonny, and Laura Greenman. "Revisiting conduct risk management in the COVID-19 era with updated DOJ criteria." *Journal of Risk Management in Financial Institutions* 13, no. 4 (2020): 295-307.

Ghatge, Aryan, Ayush Pandey, Shubham Bagul, Abhijeet Dhopare, and Geeta S. Navale. "Automation in the KYC Process." In *International Conference on ICT for Sustainable Development*, pp. 419-427. Cham: Springer Nature Switzerland, 2025.

Gilmore, William C. *Dirty money: The evolution of money laundering counter-measures*. Vol. 2. Strasbourg: Council of Europe Publishing, 1999.

Government Regulation No. 43 of 2015 on *Reporting Parties in the Prevention and Eradication of the Crime of Money Laundering.*

Hannan, Md Abdul, Md Atik Shahriar, Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad Shahriar Rahman. "A systematic literature review of blockchain-based e-KYC systems." *Computing* (2023): 1.

Jafarnejad, Sasan, François Robinet, and Raphaël Frank. "A risk-based AML framework: Finding associates through ultimate beneficial owners." In *2024 IEEE Symposium on Computational Intelligence for Financial Engineering and Economics (CIFEr)*, pp. 1-7. IEEE, 2024.

Jamil, Ainul Huda, Zuraidah Mohd-Sanusi, Yusarina Mat-Isa, and Najihah Marha Yaacob. "Money laundering risk judgement by compliance officers at financial institutions in Malaysia: the effects of customer risk determinants and regulatory enforcement." *Journal of Money Laundering Control* 26, no. 3 (2023): 535-552.

Jayapal, Cynthia, and Harish Kumar RB. "Enhancing KYC Efficiency and Accuracy Through Session Recording and Document Auto-Capture." In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, pp. 1-7. IEEE, 2023.

Johora, Fatema Tuz, Rakibul Hasan, Sayeda Farjana Farabi, Mohammad Zahidul Alam, Imran Sarkar, and Abdullah Al Mahmud. "AI advances: Enhancing banking security with fraud detection." In *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)*, pp. 289-294. IEEE, 2024.

Kaprinis, Kosmas. "Internal compliance, risk management, and their impact on culture in financial firms." In *Corporate Governance and Culture in Financial Institutions*, pp. 262-284. Edward Elgar Publishing, 2025.

Karadag, Bulut, A. Halim Zaim, and Akhan Akbulut. "Blockchain-based KYC model for credit allocation in banking." *IEEE Access* 12 (2024): 80176-80182.

Kirss, Kristin Kamilla, and Fredrik Milani. "Using Blockchain Technology to Redesign Know-Your-Customer Processes Within the Banking Industry." In *International Conference on Business Process Management*, pp. 251-262. Cham: Springer International Publishing, 2020.

Komariyah, Fitri. "Penerapan Prinsip Know Your Customer (KYC) dalam Mencegah Tindak Pidana Pencucian Uang." *Jurnal Manajemen dan Administrasi Bisnis (JUMASIS)* 1, no. 2 (2025): 58-63.

Kommadi, By Bhagvan. "Blockchain–An Elixir for Anti-Money Laundering?." *The PayTech Book: The Payment Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries* (2019): 129-131.

Korejo, Muhammad Saleem, Ramalinggam Rajamanickam, and Muhamad Helmi Md. Said. "The concept of money laundering: a quest for legal definition." *Journal of Money Laundering Control* 24, no. 4 (2021): 725-736.

Kumar, C. Vinoth, Poongundran Selvaprabhu, Nivetha Baska, U. Vivek Menon, Vinoth Babu Kumaravelu, Sunil Chinnadurai, and Farman Ali. "Ethereum blockchain framework enabling banks to know their customers." *IEEE Access* 12 (2024): 101356-101365.

Law No. 10 of 1998 on *Amendments to Law No. 7 of 1992 on Banking*.

Law No. 21 of 2011 *on the Financial Services Authority*.

Law No. 8 of 2010 on *Prevention and Eradication of the Crime of Money Laundering*.

Lekhaa, T. R., and N. Ramya Devi. "Streamlining KYC Processes for Banks with Centralized Information Repository Using Design Thinking." In *International Conference on Big Data Innovation for Sustainable Cognitive Computing*, pp. 123-132. Cham: Springer Nature Switzerland, 2023.

Levi, Michael, and Peter Reuter. "Money laundering." *Crime and justice* 34, no. 1 (2006): 289-375.

Lu, Longjie. "Regulating ESG rating firms as the gatekeepers for sustainable finance." *Capital Markets Law Journal* 19, no. 2 (2024): 184-206.

Meiryani, Meiryani, Gatot Soepriyanto, and Jessica Audrelia. "Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing." *Journal of Money Laundering Control* 26, no. 4 (2023): 892-908.

Meiryani. "Prevention and control of money laundering crimes on know your customer principles application: empirical study of Indonesia banking sector." *Journal of Money Laundering Control* 27, no. 5 (2024): 873-885.

Nawaah, Donkor, and Rockson Mintah. "AI Applications for Anti-Money Laundering and Compliance in Financial Institutions." In *Foundations of Artificial Intelligence in Finance*, pp. 149-156. Chapman and Hall/CRC.

OJK Regulation No. 12/POJK.01/2017 on *Implementation of Anti-Money Laundering and Prevention of Terrorism Financing Programs in the Financial Services Sector*.

OJK Regulation No. 39/POJK.03/2019 on *Anti-Fraud Strategy Implementation for Commercial Banks.*

Oliveira, Jose Ricardo, and Adriano Galindo Leal. "Enhancing anti-money laundering protocols: Employing machine learning to minimise false positives and improve operational cost efficiency." In *Proceedings of the 2024 8th International Conference on Advances in Artificial Intelligence*, pp. 8-13. 2024.

Ostern, Nadine Kathrin, and Johannes Riedel. "Know-your-customer (KYC) requirements for initial coin offerings." *Business & Information Systems Engineering* 63, no. 5 (2021): 551-567.

Patil, Pradnya, and M. Sangeetha. "Blockchain-based decentralized KYC verification framework for banks." *Procedia Computer Science* 215 (2022): 529-536.

Pereira, José Lino, Afshin Ashofteh, and Ian Scott. "Blockchain for Know Your Customer Process in Anti-money Laundering Compliance: A Review in Financial Services." In *Iberian Conference on Information Systems and Technologies*, pp. 110-120. Cham: Springer Nature Switzerland, 2025.

Pocher, Nadia, Mirko Zichichi, Fabio Merizzi, Muhammad Zohaib Shafiq, and Stefano Ferretti. "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics." *Electronic Markets* 33, no. 1 (2023): 37.

PPATK Regulation No. 9 of 2017 *on Procedures for Submission of Information on PPATK Examination Results to Investigators.*

Raj, Mahima, Hadiya Khan, Samta Kathuria, Yerrolla Chanti, and Mansi Sahu. "The use of artificial intelligence in anti-money laundering (AML)." In *2024 3rd International conference on sentiment analysis and deep learning (ICSADL)*, pp. 272-277. IEEE, 2024.

Reuter, Peter. *Chasing dirty money: The fight against money laundering*. Peterson Institute, 2005.

Riccardi, Michele, and Peter Reuter. "The varieties of money laundering and the determinants of offender choices." *European Journal on Criminal Policy and Research* 30, no. 3 (2024): 333-358.

Rusanov, Georgy, and Yury Pudovochkin. "Money laundering in the modern crime system." *Journal of money laundering control* 24, no. 4 (2021): 860-868.

Santoso, Budi, David ML Tobing, and Zico Junius Fernando. "Know Your Customer (KYC) Model: A Legal Reform Strategy to Prevent Abuse of Financial Services in Child Sexual Exploitation Transactions." *Journal of Law and Legal Reform* 6, no. 1 (2025): 239-264.

Scarcella, Giovanni. "Qui tam and the bank secrecy act: a Public-Private enforcement model to improve anti-Money laundering efforts." *Fordham L. Rev.* 90 (2021): 1359.

Sharairi, Mohammad Haroun. "Mapping Conceptual Frameworks for Real Time Fraud Risk Management in Digital Microfinance." *Enterprise Development and Microfinance* 35, no. 1 (2025): 302-318.

Simanjuntak, Effendi Lod. *Penegakan Hukum Pencucian Uang Lintas Negara, Teori dan Praksis Penerapan MLA di ASEAN*. Yogyakarta: Arti Bumi Intaran, 2022.

Somda, Metouole Mwinbe Yves Ghislain, Samuel Ouya, and Gervais Mendy. "Implementation of Robotic Process Automation To Decrease the Time Requires For KYC Onboarding Process." In *2023 6th International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pp. 345-350. IEEE, 2023.

Sumanti, N., and Madhavi Damle. "Transforming the KYC Process in Banking: Using Hyperautomation to Enhance Efficiency and Security." In *2025 International Conference on Technology Enabled Economic Changes (InTech)*, pp. 1217-1224. IEEE, 2025.

Tuba, Maphuti, and Chinelle Van der Westhuizen. "An analysis of the 'know your customer'policy as an effective tool to combat money laundering: is it about who or what to know that counts?." *International Journal of Public Law and Policy* 4, no. 1 (2014): 53-70.

van Solinge, Tim Boekhout. "Drugs and money: Managing the drug trade and crime-money in Europe." (2007): 698-701.

Von Haenisch, Hans-Joachim, and Thomas Egner. "Know your customer: Unravelling the challenges." *Journal of Payments Strategy & Systems* 18, no. 1 (2024): 30-38.

Wongkar, Kanon Mommsen. "Implementation of KYC Principles for Indonesian Payment Services Provider." *Journal of Accounting, Business and Management (JABM)* 32, no. 1 (2024): 208-217.

Wood, Jenny. *Global business practises*. EuroAsia Semiconductor, 2012.

Xiong, Xihan, Michael Huth, and William Knottenbelt. "REGKYC: Supporting privacy and compliance enforcement for KYC in blockchains." In *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1-5. IEEE, 2025.