Jurnal Sahabat ISNU-SU (JSISNU)
(eISSN: 3064-0067)
Volume 3, Nomor 1, Mei 2026 (01-18)

Strengthening Integrated Financial Crime Enforcement in Indonesia: Evaluating the Institutional Synergy Between the Financial Services Authority (OJK) and the Indonesian Financial Intelligence Unit (PPATK)

Farhan Fathur Rahman[1], Indah Sari Br. Barus[2], Qori Asvifah Bintang[3], Rafly Alikhsan Sikumbang[4]
[1]Universitas Islam Negeri Sunan Kalijaga Yogyakarta
[234]Universitas Islam Negeri Sumatera Utara
E-mail: 22203011040@uin-suka.ac.id indah020623104@uinsu.ac.id qori0206232054@uinsu.ac.id raflysikumbang120@gmail.com

Info Articles

Article History
Received: 2026-05-16
Revised: 2026-05-24
Published: 2026-05-30

Keywords:
Banking Crimes; OJK, PPATK; Money Laundering; Special Criminal Law

Abstract

The rapid transformation of the banking sector through digital financial services has significantly increased the complexity of banking crimes, extending beyond conventional fraud to sophisticated forms of financial misconduct, including cyber-enabled banking fraud, cross-border money laundering, beneficial ownership concealment, and illicit financial flows. These developments have challenged the effectiveness of traditional banking supervision and criminal law enforcement mechanisms. This study aims to critically examine the institutional relationship between the Financial Services Authority (Otoritas Jasa Keuangan/OJK) and the Indonesian Financial Transaction Reports and Analysis Center (Pusat Pelaporan dan Analisis Transaksi Keuangan/PPATK) in combating banking crimes under the Indonesian legal framework. Employing normative legal research, this study applies statutory, conceptual, analytical, and comparative approaches by examining Indonesian banking legislation alongside international standards concerning financial supervision and anti-money laundering issued by the Financial Action Task Force (FATF) and other international institutions. The findings demonstrate that although OJK and PPATK possess distinct legal mandates, the effectiveness of banking crime enforcement largely depends on institutional coordination rather than individual institutional authority. OJK performs prudential regulation and supervisory functions aimed at preventing systemic risks and ensuring regulatory compliance within the banking sector, whereas PPATK functions as Indonesia's Financial Intelligence Unit (FIU) responsible for collecting, analyzing, and disseminating financial intelligence associated with suspicious financial transactions. Nevertheless, overlapping supervisory responsibilities, fragmented regulatory coordination, delayed information exchange, and the absence of an integrated financial crime governance mechanism continue to impede effective law enforcement. This study proposes an Integrated Financial Crime Enforcement Model that emphasizes real-time institutional coordination, regulatory harmonization, intelligence-based supervision, and collaborative asset recovery as strategic measures to strengthen Indonesia's financial integrity. The proposed model contributes to the development of banking law by integrating prudential supervision and financial intelligence into a comprehensive institutional framework capable of responding to increasingly sophisticated financial crimes.

I. INTRODUCTION

The banking sector constitutes one of the most fundamental pillars of modern economic development by facilitating financial intermediation, mobilizing public savings, supporting investment, and ensuring the circulation of capital necessary for sustainable national growth. As financial markets become increasingly interconnected through globalization and digital transformation, banking institutions are no longer merely financial intermediaries but have evolved into strategic infrastructures supporting domestic and international economic activities. Consequently, maintaining the integrity, transparency, and stability of banking institutions has become an essential objective of every legal system seeking to promote economic resilience and public confidence. Banking stability is therefore inseparable from the effectiveness of legal institutions responsible for regulating, supervising, and enforcing compliance within the financial sector. Banking crimes not only generate substantial economic losses for financial institutions and customers but also undermine market confidence, threaten macroeconomic stability, and potentially facilitate transnational organized crime through the movement of illicit financial assets. Therefore, banking crime should no longer be understood solely as an ordinary economic offense but rather as a multidimensional threat to financial governance and national economic security (Nelson, 2017).

The increasing sophistication of financial technology has fundamentally transformed the nature of banking crimes worldwide. Conventional banking offenses such as embezzlement, fictitious lending, forgery of banking documents, and abuse of authority have gradually evolved into highly organized financial crimes involving cyber-enabled fraud, identity theft, shell corporations, digital payment manipulation, cryptocurrency laundering, trade-based money laundering, and cross-border illicit financial flows. These crimes frequently exploit regulatory disparities across jurisdictions while utilizing complex financial structures that make asset tracing increasingly difficult. As financial criminals adopt innovative technologies comparable to those employed by legitimate financial institutions, conventional supervisory mechanisms become progressively inadequate. Consequently, banking supervision has shifted from a purely compliance-oriented approach toward intelligence-based supervision capable of detecting hidden financial risks before substantial financial losses occur. This transformation has encouraged jurisdictions worldwide to strengthen cooperation between banking supervisors and financial intelligence units as an integrated strategy against financial crimes.

Indonesia faces similar challenges arising from the rapid expansion of digital banking services, financial technology innovation, and increasing international financial transactions. While financial inclusion has improved significantly over the past decade, the expansion of banking services has simultaneously created new opportunities for sophisticated financial crimes that extend beyond the regulatory capacity of traditional supervisory institutions. Banking crimes in Indonesia are no longer limited to violations expressly regulated under Articles 46 through 50A of Law Number 10 of 1998 concerning Banking but increasingly intersect with money laundering, corruption, cybercrime, terrorism financing, tax evasion, and organized financial fraud. The interrelationship among these offenses demonstrates that banking crimes should be examined within a broader financial crime framework rather than through a narrow interpretation of banking regulations alone. Such complexity requires integrated institutional cooperation capable of combining prudential supervision, financial intelligence, criminal investigation, and asset recovery within a unified legal framework.

Indonesia has established two principal institutions responsible for safeguarding the integrity of its financial system. The Financial Services Authority (Otoritas Jasa Keuangan—OJK) exercises regulatory and supervisory authority over banking institutions through prudential regulation, risk-based supervision, corporate governance oversight, and consumer protection. Meanwhile, the Financial Transaction Reports and Analysis Center (Pusat Pelaporan dan Analisis Transaksi Keuangan—PPATK) serves as Indonesia's Financial Intelligence Unit (FIU), entrusted with receiving, analyzing, and disseminating financial intelligence relating to suspicious financial transactions in accordance with the anti-money laundering and counter-terrorism financing regime. Although these institutions possess distinct statutory mandates, both ultimately pursue the same objective of maintaining financial integrity and preventing financial crimes from threatening national economic stability. Their institutional relationship therefore represents a critical component of Indonesia's financial governance architecture.

Despite the existence of comprehensive legal regulations governing banking supervision and anti-money laundering, practical implementation continues to encounter significant institutional challenges. Information exchange between supervisory authorities and criminal law enforcement agencies often remains fragmented, overlapping supervisory competencies occasionally create regulatory uncertainty, while administrative supervision and criminal investigation frequently operate within separate institutional frameworks. Such fragmentation may delay early detection of suspicious financial activities, reduce the effectiveness of preventive supervision, and ultimately weaken asset recovery efforts following the commission of financial crimes. Consequently, the effectiveness of banking crime enforcement cannot be assessed solely by examining the legal authority of individual institutions but must instead be evaluated through the quality of institutional coordination, regulatory harmonization, and intelligence sharing among financial regulatory bodies.

Previous legal studies concerning banking crimes in Indonesia have predominantly concentrated on the interpretation of banking criminal provisions, anti-money laundering legislation, or the respective institutional authorities of OJK and PPATK. Although these studies provide valuable doctrinal understanding, relatively limited attention has been devoted to evaluating how institutional synergy between prudential supervision and financial intelligence contributes to integrated financial crime enforcement. Existing scholarship generally examines OJK and PPATK independently rather than analyzing their complementary functions within a unified governance framework capable of addressing increasingly sophisticated financial crimes. Accordingly, a significant research gap remains regarding the institutional integration necessary to strengthen financial crime enforcement under Indonesia's evolving financial regulatory system.

This study seeks to address that gap by evaluating the effectiveness of institutional coordination between OJK and PPATK within Indonesia's banking law framework while proposing an Integrated Financial Crime Enforcement Model designed to strengthen regulatory cooperation, intelligence sharing, supervisory effectiveness, and asset recovery mechanisms. Unlike previous studies that primarily describe institutional authority from a normative perspective, this research develops a conceptual framework integrating prudential banking supervision and financial intelligence into a comprehensive legal strategy capable of responding to emerging financial crime risks in the digital banking era. Accordingly, this study contributes not only to the development of Indonesian banking law but also to broader discussions concerning institutional governance, financial regulation, and anti-money laundering policies in emerging economies.

II. RESEARCH METHODS

This study employs normative legal research with an evaluative and comparative orientation to examine the effectiveness of institutional coordination in combating banking crimes within Indonesia's financial regulatory framework. Unlike conventional doctrinal legal research, which merely interprets statutory provisions, this study combines statutory analysis with conceptual, comparative, and analytical legal approaches to evaluate whether the current institutional arrangement between the Financial Services Authority (OJK) and the Indonesian Financial Transaction Reports and Analysis Center (PPATK) adequately responds to the increasing complexity of modern financial crimes. Through this multidimensional approach, the study seeks not only to identify the applicable legal norms but also to assess their institutional implementation and formulate recommendations for strengthening integrated financial crime governance.

The statutory approach examines the principal legal instruments governing banking supervision, financial intelligence, anti-money laundering, and criminal law enforcement in Indonesia. These include Law Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998, Law Number 21 of 2011 concerning the Financial Services Authority, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law), and implementing regulations issued by OJK and PPATK relating to risk management, anti-money laundering (AML), and counter-terrorism financing (CFT). These statutory materials are analyzed systematically to identify the legal distribution of authority, supervisory responsibilities, and institutional mechanisms established to combat banking crimes (Butt, 2018).

The conceptual approach explores contemporary legal theories relating to banking regulation, financial governance, financial intelligence, institutional accountability, risk-based supervision, and integrated law enforcement. Particular attention is given to the evolution of banking supervision from traditional compliance-oriented regulation toward intelligence-led supervision, which increasingly relies upon financial information analysis, suspicious transaction reporting, and preventive risk assessment. The study further incorporates concepts developed by international financial organizations, including the Financial Action Task Force (FATF), the Basel Committee on Banking Supervision (BCBS), the Egmont Group of Financial Intelligence Units, and the Organisation for Economic Co-operation and Development (OECD), to evaluate Indonesia's regulatory framework against internationally accepted standards (FATF, 2023; Basel Committee on Banking Supervision, 2024).

A comparative legal approach is employed to examine institutional coordination models adopted by several jurisdictions recognized for implementing advanced financial crime enforcement systems. Comparative observations focus primarily on Singapore, Australia, the United Kingdom, and the European Union, where banking supervisors maintain structured cooperation with Financial Intelligence Units (FIUs) through integrated information-sharing mechanisms, joint supervisory arrangements, and coordinated asset recovery procedures. Rather than conducting a comprehensive comparative analysis of foreign legal systems, these jurisdictions serve as analytical references for identifying institutional best practices relevant to Indonesia's legal reform.

The analytical approach evaluates the effectiveness of institutional interaction between OJK and PPATK by examining the legal relationship among supervisory authority, financial intelligence, criminal investigation, and administrative enforcement. Legal norms are interpreted through qualitative legal reasoning using deductive analysis, beginning with general legal principles concerning financial regulation and concluding with specific institutional implications for banking crime enforcement in Indonesia. This approach enables the study to identify legal inconsistencies, overlapping authorities, regulatory fragmentation, and institutional weaknesses that potentially reduce the effectiveness of banking crime prevention.

The legal materials employed consist of primary, secondary, and tertiary legal sources. Primary legal materials include legislation, government regulations, OJK regulations, PPATK regulations, Constitutional Court decisions where relevant, and other legally binding instruments governing banking supervision and financial intelligence. Secondary legal materials comprise scholarly books, peer-reviewed international journal articles indexed in Scopus, legal commentaries, official reports issued by FATF, Basel Committee, IMF, World Bank, OECD, and Egmont Group, together with academic publications discussing banking crimes, anti-money laundering, financial governance, and institutional cooperation. Tertiary legal materials include legal dictionaries, encyclopedias, and authoritative reference sources that assist in clarifying legal terminology and conceptual interpretation.

The collected legal materials are analyzed qualitatively through legal interpretation, conceptual synthesis, comparative evaluation, and critical normative assessment. Rather than merely describing existing legislation, the analysis seeks to determine whether Indonesia's current institutional framework sufficiently accommodates the increasingly sophisticated characteristics of banking crimes occurring within digital financial ecosystems. The final stage of analysis develops an Integrated Financial Crime Enforcement Model, intended as a conceptual framework for strengthening institutional coordination between prudential banking supervision and financial intelligence in order to improve financial crime prevention, law enforcement, and asset recovery.

III. RESULTS AND DISCUSSION

A. Definition and Classification of Banking Crim The Evolution of Banking Crimes within the Digital Financial Ecosystem

The transformation of the global financial system has fundamentally altered both the characteristics and complexity of banking crimes. Historically, banking crimes were generally associated with relatively conventional offenses, including embezzlement of customer funds, document forgery, fictitious credit facilities, illegal banking operations, and violations of banking secrecy. These offenses primarily occurred within the internal operational structure of banking institutions and were therefore addressed through conventional supervisory mechanisms emphasizing administrative compliance and prudential regulation. However, rapid technological innovation has significantly expanded the operational environment of banks, creating increasingly sophisticated opportunities for financial criminals to exploit digital infrastructures, international payment systems, electronic banking platforms, and cross-border financial networks (Levi & Reuter, 2006).

The digitalization of banking services has substantially improved financial inclusion, operational efficiency, and customer convenience. Nevertheless, digital banking simultaneously creates new vulnerabilities that cannot be adequately addressed through traditional supervisory models. Cyber-enabled fraud, identity theft, phishing attacks, unauthorized electronic fund transfers, synthetic identities, cryptocurrency laundering, shell corporations, beneficial ownership concealment, and trade-based money laundering have become integral components of contemporary banking crimes. Unlike conventional banking offenses, these crimes frequently involve multiple jurisdictions, sophisticated technological infrastructures, anonymous financial transactions, and organized criminal networks capable of exploiting differences among national regulatory systems (UNODC, 2022).

Consequently, banking crimes should no longer be interpreted narrowly as violations of banking regulations alone. Contemporary banking crimes constitute part of a broader financial crime ecosystem involving corruption, tax evasion, money laundering, terrorist financing, cybercrime, corporate fraud, securities violations, and illicit financial flows. Financial institutions increasingly serve as conduits through which proceeds of crime are disguised, transferred, layered, and ultimately integrated into legitimate economic activities. Accordingly, banking law enforcement has shifted from a reactive criminal justice approach toward preventive financial governance emphasizing risk identification, intelligence gathering, institutional cooperation, and continuous financial monitoring (FATF, 2023).

Within Indonesian law, banking crimes remain primarily regulated under Articles 46 through 50A of Law Number 10 of 1998 concerning Banking. These provisions criminalize unauthorized banking activities, violations of banking secrecy, manipulation of banking records, abuse of authority by bank management, and unlawful conduct involving affiliated parties and controlling shareholders. Although these statutory provisions continue to provide the principal legal basis for prosecuting banking offenses, they were largely formulated during an era in which digital financial services had not yet fundamentally transformed banking operations. Consequently, many contemporary financial crimes occurring through digital banking infrastructures intersect simultaneously with legislation governing cybercrime, anti-money laundering, corruption, financial technology, and electronic information systems.

The emergence of integrated financial crimes illustrates that the legal protection of banking institutions cannot rely solely upon criminal sanctions imposed after financial losses occur. Instead, effective banking crime prevention requires continuous institutional supervision capable of detecting suspicious financial behavior before criminal proceeds become fully integrated into the financial system. This preventive orientation has become the dominant paradigm within international financial regulation, emphasizing risk-based supervision, customer due diligence, beneficial ownership transparency, suspicious transaction reporting, and intelligence-led financial monitoring as essential components of financial integrity (Basel Committee on Banking Supervision, 2024).

Indonesia has gradually adopted this preventive regulatory philosophy through the establishment of OJK as the integrated financial services supervisor and PPATK as the national Financial Intelligence Unit. Nevertheless, institutional effectiveness depends not merely upon the existence of these organizations but rather upon the extent to which prudential supervision and financial intelligence function as complementary components within a unified financial crime governance framework. The following sections therefore examine the respective institutional roles of OJK and PPATK while critically evaluating the effectiveness of their coordination in combating increasingly sophisticated banking crimes.

B. The Regulatory Authority of the Financial Services Authority (OJK): From Prudential Supervision to Risk-Based Financial Governance

The establishment of the Financial Services Authority (Otoritas Jasa Keuangan/OJK) marked a fundamental transformation in Indonesia's financial regulatory architecture by replacing the fragmented supervisory model previously divided between Bank Indonesia and several sectoral authorities. Through Law Number 21 of 2011 concerning the Financial Services Authority, Indonesia adopted an integrated supervisory framework intended to ensure that regulation and supervision of banking, capital markets, insurance, pension funds, financing institutions, and other financial services operate within a single institutional structure. This institutional reform reflects an international regulatory trend emphasizing integrated financial supervision as an essential mechanism for maintaining financial system stability, protecting consumers, and mitigating systemic risks arising from increasingly interconnected financial markets (Butt, 2018).

Unlike conventional banking regulators whose supervisory functions primarily focus on ensuring compliance with statutory provisions, OJK has gradually adopted a risk-based supervisory approach that evaluates the overall risk profile of financial institutions rather than merely identifying formal legal violations. Under this approach, banking supervision is no longer limited to determining whether banks comply with regulatory obligations but extends to assessing governance quality, capital adequacy, liquidity resilience, operational risk management, cybersecurity readiness, anti-money laundering compliance, technological innovation, and enterprise-wide risk management. Consequently, the effectiveness of banking supervision depends not only upon legal enforcement but also upon the institutional capacity to identify emerging risks before they materialize into financial crimes or systemic failures (Basel Committee on Banking Supervision, 2024).

The legal authority of OJK encompasses regulatory functions, licensing authority, prudential supervision, administrative enforcement, consumer protection, and institutional governance oversight. These functions collectively establish OJK as the primary gatekeeper responsible for maintaining the integrity of Indonesia's banking sector. Prudential supervision conducted by OJK requires banks to continuously implement Good Corporate Governance (GCG), maintain adequate capital buffers, strengthen internal control mechanisms, implement enterprise risk management, and ensure compliance with Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) obligations. In practice, these supervisory responsibilities are expected to reduce opportunities for banking crimes by strengthening institutional accountability before criminal conduct occurs (OJK Regulation No. 12/POJK.03/2021).

One of the most significant developments in contemporary banking supervision is the recognition that financial crimes often originate from weaknesses in institutional governance rather than isolated criminal intent. Numerous banking scandals demonstrate that fraudulent lending, embezzlement of customer assets, accounting manipulation, insider abuse, and illicit financial transactions frequently occur because corporate governance structures fail to function effectively. Weak internal controls, inadequate compliance culture, ineffective boards of commissioners, conflicts of interest, and insufficient audit mechanisms collectively create an institutional environment conducive to financial misconduct. Consequently, prudential supervision increasingly emphasizes governance quality as a preventive instrument of criminal law enforcement rather than merely an administrative regulatory requirement (Coffee, 2006).

The implementation of Good Corporate Governance (GCG) therefore constitutes one of OJK's most important preventive strategies in combating banking crimes. Governance principles such as transparency, accountability, responsibility, independence, and fairness reduce opportunities for regulatory arbitrage while increasing institutional accountability throughout banking operations. Banks maintaining effective governance structures generally demonstrate stronger compliance cultures, greater transparency in financial reporting, improved internal audit systems, and enhanced resistance against fraud and money laundering schemes. Conversely, governance failures frequently precede major banking crimes because organizational weaknesses facilitate concealment of illicit financial activities.

However, despite the extensive legal authority granted to OJK, prudential supervision alone remains insufficient to address increasingly sophisticated financial crimes. Modern financial criminals rarely operate exclusively within regulated banking activities. Instead, they utilize interconnected financial instruments involving shell corporations, nominee arrangements, offshore jurisdictions, digital payment systems, virtual assets, and complex cross-border transactions specifically designed to obscure beneficial ownership and conceal criminal proceeds. Such sophisticated financial structures often remain undetectable through conventional supervisory examinations because formal regulatory compliance does not necessarily reveal underlying criminal intentions.

This limitation demonstrates that prudential supervision possesses inherent institutional boundaries. OJK primarily evaluates whether financial institutions comply with applicable regulations and maintain sound governance practices. Nevertheless, compliance supervision differs fundamentally from financial intelligence analysis. A bank may satisfy prudential regulatory requirements while simultaneously facilitating suspicious financial transactions whose criminal characteristics become identifiable only after extensive financial analysis. Consequently, prudential supervision cannot independently perform the intelligence functions necessary to detect hidden money laundering networks, organized financial crime, terrorism financing, or complex illicit financial flows.

The increasing sophistication of banking crimes has therefore transformed OJK's institutional role from a traditional banking regulator into a strategic component of Indonesia's broader financial crime prevention system. Rather than functioning exclusively as an administrative supervisory authority, OJK increasingly contributes to early detection of financial crimes through risk assessment, regulatory oversight, governance supervision, compliance evaluation, and institutional monitoring. Nevertheless, effective criminal law enforcement ultimately requires complementary cooperation with institutions possessing specialized financial intelligence capabilities. This institutional necessity explains why coordination between OJK and PPATK has become increasingly indispensable within Indonesia's contemporary financial governance framework.

From a broader regulatory perspective, the effectiveness of OJK should no longer be measured solely by the number of supervisory inspections conducted or administrative sanctions imposed upon financial institutions. Instead, institutional performance should also be evaluated according to its capacity to contribute toward early detection of suspicious financial behavior, prevention of systemic financial risks, enhancement of regulatory compliance, and coordination with financial intelligence agencies responsible for tracing illicit financial flows. Such performance indicators better reflect contemporary international standards emphasizing preventive financial governance rather than reactive regulatory enforcement.

Accordingly, OJK should be understood not merely as Indonesia's banking supervisor but as an integral component of a preventive financial crime governance system. Its supervisory authority constitutes the first institutional barrier protecting the banking sector from financial crimes. Nevertheless, prudential supervision alone cannot adequately identify sophisticated criminal financial activities without support from financial intelligence analysis. Therefore, institutional cooperation between OJK and PPATK becomes a legal necessity rather than an administrative preference. The effectiveness of Indonesia's banking crime enforcement ultimately depends upon the successful integration of prudential supervision with intelligence-led financial investigation.

C. PPATK as Indonesia's Financial Intelligence Unit: Intelligence-Led Law Enforcement Against Banking Crimes

The increasing sophistication of financial crimes has fundamentally transformed the philosophy of criminal law enforcement within the banking sector. Traditionally, criminal investigations relied heavily upon physical evidence, witness testimony, documentary records, and the identification of offenders after criminal conduct had occurred. However, globalization, digital banking, financial technology, and cross-border financial transactions have significantly reduced the effectiveness of conventional investigative methods. Criminal organizations increasingly exploit the complexity of financial systems to conceal illicit proceeds through multiple layers of transactions that frequently involve several financial institutions and jurisdictions. Consequently, modern financial crime enforcement has shifted toward an intelligence-led approach that prioritizes early detection of suspicious financial behavior before criminal proceeds become fully integrated into the legitimate economy (Levi & Reuter, 2006).

Within this paradigm, Financial Intelligence Units (FIUs) have emerged as indispensable institutions responsible for transforming financial transaction data into actionable intelligence capable of supporting criminal investigations, regulatory supervision, and asset recovery. Unlike conventional law enforcement agencies, FIUs do not primarily investigate criminal suspects or prosecute offenders. Rather, they function as specialized analytical institutions that collect, process, analyze, and disseminate financial information relating to suspicious financial activities. Their principal objective is to identify hidden financial patterns that may indicate money laundering, corruption, tax evasion, terrorism financing, banking fraud, organized crime, or other predicate offences before these activities generate irreversible economic consequences (FATF, 2023).

Indonesia established the Financial Transaction Reports and Analysis Center (Pusat Pelaporan dan Analisis Transaksi Keuangan PPATK) as its national Financial Intelligence Unit under Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering. The creation of PPATK reflects Indonesia's commitment to implementing international anti-money laundering standards developed by the Financial Action Task Force (FATF) and the Egmont Group of Financial Intelligence Units. Rather than functioning solely as a reporting agency, PPATK represents the central institution responsible for generating financial intelligence that bridges financial supervision and criminal law enforcement. Accordingly, its institutional significance extends far beyond administrative compliance because financial intelligence constitutes the earliest source of information concerning illicit financial activities occurring within the banking system.

The institutional philosophy underlying PPATK differs fundamentally from conventional criminal investigations. Criminal investigations generally follow the principle of "follow the suspect," whereby investigators identify offenders before tracing the criminal conduct committed. Financial intelligence, by contrast, adopts the doctrine of "follow the money," which assumes that every significant criminal activity ultimately produces financial transactions capable of being identified, analyzed, and reconstructed through systematic examination of financial records. Under this doctrine, money itself becomes the primary source of evidence because illicit financial flows frequently reveal criminal networks more accurately than witness testimony or confessions. Consequently, financial intelligence enables law enforcement agencies to uncover complex criminal organizations whose operational structures remain intentionally concealed from traditional investigative methods (Gilmore, 2011).

The operational effectiveness of PPATK depends upon what international literature describes as the Financial Intelligence Cycle, comprising four interconnected stages: collection, analysis, dissemination, and operational utilization. The first stage involves collecting financial information from reporting entities, including banks, insurance companies, securities firms, fintech providers, and other financial service institutions obligated to submit Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), international fund transfer reports, and additional financial information required under anti-money laundering legislation. These reporting obligations establish the informational foundation necessary for identifying abnormal financial behavior that may indicate criminal activity.

The second stage consists of financial analysis, representing the core institutional function of PPATK. Rather than mechanically reviewing transaction reports, PPATK applies strategic financial analysis to identify transaction patterns inconsistent with customers' economic profiles, business activities, or historical financial behavior. Advanced analytical techniques permit the reconstruction of complex financial networks involving nominee accounts, shell corporations, beneficial ownership structures, layered transactions, trade-based money laundering, digital assets, and cross-border transfers specifically designed to conceal the origin of illicit proceeds. Financial analysis therefore transforms raw transactional data into structured financial intelligence capable of revealing criminal patterns invisible through ordinary banking supervision.

The third stage involves dissemination of intelligence products to competent authorities responsible for conducting criminal investigations, administrative supervision, taxation, corruption eradication, customs enforcement, or other legal proceedings. Importantly, PPATK does not determine criminal liability because its analytical products do not constitute judicial findings of guilt. Instead, financial intelligence functions as strategic preliminary information supporting investigative decision-making by competent law enforcement agencies. The distinction between financial intelligence and criminal evidence preserves due process while simultaneously enhancing investigative efficiency by directing investigators toward financial activities requiring further examination.

The final stage concerns operational utilization, whereby financial intelligence supports criminal investigations, prosecution, confiscation of criminal assets, international legal cooperation, and judicial proceedings. Increasingly, financial intelligence also contributes to preventive regulatory supervision because suspicious financial patterns frequently reveal institutional weaknesses within banking governance long before criminal prosecutions commence. Consequently, financial intelligence has evolved beyond a purely investigative instrument into an essential component of preventive financial governance.

One of the most significant contributions of PPATK lies in strengthening the implementation of risk-based Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) supervision. International regulatory standards no longer require financial institutions merely to report suspicious transactions. Instead, banks must continuously identify customers presenting elevated money laundering risks through enhanced customer due diligence, ongoing transaction monitoring, beneficial ownership verification, politically exposed person (PEP) identification, sanctions screening, and continuous risk assessment. PPATK provides strategic guidance enabling financial institutions to recognize emerging typologies of financial crimes, thereby improving the quality of suspicious transaction reporting submitted by reporting entities.

Nevertheless, the effectiveness of PPATK cannot be measured solely by the number of Suspicious Transaction Reports received annually. A high reporting volume does not necessarily indicate successful financial intelligence if analytical products fail to generate operational outcomes, criminal prosecutions, asset recovery, or preventive regulatory reforms. Accordingly, international best practices increasingly evaluate Financial Intelligence Units according to intelligence quality, analytical capability, inter-agency cooperation, timeliness of information dissemination, technological capacity, and measurable contributions to financial crime disruption rather than purely quantitative reporting statistics (Egmont Group, 2023).

Despite its strategic institutional position, PPATK encounters significant challenges arising from the rapidly changing nature of financial crime. Digital banking, virtual assets, decentralized finance (DeFi), anonymous payment technologies, cross-border electronic transfers, and increasingly sophisticated beneficial ownership arrangements have expanded the complexity of financial intelligence analysis. Criminal organizations frequently employ professional intermediaries, offshore corporate structures, and emerging financial technologies specifically designed to obscure ownership and transaction histories. Consequently, maintaining effective financial intelligence requires continuous technological innovation, advanced analytical methodologies, international information exchange, and institutional cooperation extending far beyond domestic regulatory boundaries.

These developments demonstrate that PPATK should no longer be perceived merely as a reporting institution operating after suspicious transactions occur. Rather, PPATK has evolved into Indonesia's strategic financial intelligence center whose analytical capability directly influences the effectiveness of banking supervision, criminal investigations, corruption eradication, asset recovery, and national financial security. Financial intelligence therefore functions as the connecting bridge between prudential banking supervision and criminal law enforcement.

However, financial intelligence alone cannot prevent banking crimes if supervisory authorities fail to integrate analytical findings into prudential oversight. Likewise, banking supervision cannot effectively detect sophisticated financial crimes without intelligence capable of identifying concealed financial behavior. This institutional interdependence confirms that neither OJK nor PPATK possesses sufficient institutional capacity to independently combat contemporary banking crimes. Instead, effective financial crime governance depends upon continuous coordination, real-time information sharing, joint risk assessment, and harmonized regulatory strategies. The following section therefore examines the institutional fragmentation that continues to limit effective cooperation between OJK and PPATK despite their complementary legal mandates.

D. Institutional Fragmentation Between OJK and PPATK: Legal Challenges in Banking Crime Enforcement

Although Indonesia has established an extensive legal framework governing banking supervision, anti-money laundering, and financial crime prevention, the effectiveness of banking crime enforcement remains constrained by institutional fragmentation rather than by the absence of legal authority. The establishment of OJK and PPATK undoubtedly represents a significant institutional reform intended to strengthen financial governance. Nevertheless, the existence of multiple supervisory institutions does not automatically produce an integrated enforcement system. Instead, fragmented institutional mandates, overlapping regulatory responsibilities, inconsistent information-sharing mechanisms, and sectoral approaches to financial supervision continue to reduce the overall effectiveness of banking crime prevention.

The primary challenge does not lie in determining which institution possesses greater authority but rather in the manner in which institutional authority is exercised within an increasingly interconnected financial environment. Contemporary banking crimes rarely fall exclusively within a single regulatory domain. A single criminal scheme may simultaneously involve violations of banking regulations, anti-money laundering obligations, corporate governance standards, taxation rules, electronic transaction laws, corruption statutes, and cybercrime legislation. Consequently, institutional responses that remain confined within sectoral legal mandates inevitably create enforcement gaps that sophisticated financial criminals are able to exploit.

From a regulatory perspective, OJK and PPATK operate under fundamentally different legal philosophies. OJK functions as a prudential supervisory authority emphasizing regulatory compliance, financial stability, institutional governance, and risk mitigation. Its primary objective is preventive supervision designed to ensure that financial institutions remain sound, solvent, and compliant with applicable regulations. PPATK, on the other hand, performs financial intelligence functions directed toward identifying suspicious financial activities, reconstructing illicit financial flows, and supporting criminal investigations. Whereas OJK evaluates institutional compliance, PPATK evaluates transactional behavior. Although these institutional functions are complementary, they frequently operate independently within separate legal and administrative frameworks.

This separation creates what institutional governance scholars describe as regulatory fragmentation, namely a condition in which multiple public institutions pursue similar public objectives through disconnected regulatory mechanisms. Regulatory fragmentation is particularly problematic within financial crime enforcement because banking supervision increasingly depends upon timely access to financial intelligence, while financial intelligence itself requires contextual information concerning banking operations, institutional governance, customer risk profiles, and prudential compliance. Delays or limitations in exchanging such information significantly reduce the capacity of both institutions to identify emerging financial threats before criminal proceeds become irrecoverable.

A further challenge concerns the asymmetrical flow of information between regulatory authorities and criminal law enforcement agencies. Although Indonesian legislation permits cooperation among OJK, PPATK, the National Police, the Attorney General's Office, the Corruption Eradication Commission (KPK), Bank Indonesia, and other competent authorities, the legal framework does not yet establish a comprehensive real-time institutional coordination mechanism capable of integrating supervisory findings, financial intelligence, investigative developments, and asset recovery measures into a unified operational platform. Consequently, institutional cooperation frequently remains reactive rather than preventive, occurring only after substantial financial losses have already materialized.

The rapid digitalization of financial services has further intensified these institutional challenges. Digital banking, mobile payment platforms, electronic wallets, peer-to-peer lending, virtual assets, and decentralized financial technologies have significantly expanded the number of financial intermediaries participating within Indonesia's financial ecosystem. Criminal organizations increasingly exploit this complexity by distributing illicit transactions across multiple financial institutions, jurisdictions, and technological platforms, thereby preventing any single supervisory institution from obtaining a complete picture of the underlying criminal network. Fragmented supervision therefore produces fragmented intelligence, allowing sophisticated financial crimes to remain undetected despite individual institutional compliance with existing legal obligations.

An additional concern relates to the legal distinction between administrative enforcement and criminal law enforcement. OJK possesses extensive authority to impose administrative sanctions upon financial institutions violating prudential regulations, including written warnings, financial penalties, business restrictions, suspension of management, and license revocation. Administrative sanctions undoubtedly contribute to strengthening regulatory compliance; however, they are not designed to dismantle organized criminal networks or recover proceeds derived from complex financial crimes. Conversely, PPATK may identify suspicious financial patterns indicating serious criminal conduct, yet it lacks prosecutorial authority to independently initiate criminal proceedings. As a consequence, banking crime enforcement inevitably depends upon coordinated action involving multiple institutions whose legal mandates remain functionally interdependent.

The complexity of institutional interaction becomes even more apparent when banking crimes involve transnational financial transactions. Money laundering schemes increasingly rely upon offshore financial centers, shell corporations, nominee shareholders, layered international transfers, digital assets, and beneficial ownership concealment. Effective investigation of such crimes requires immediate international cooperation among Financial Intelligence Units, banking supervisors, customs authorities, taxation agencies, prosecutors, and international law enforcement organizations. Although PPATK actively participates within the Egmont Group and various international cooperation mechanisms, the effectiveness of cross-border financial intelligence remains closely linked to the quality of domestic institutional coordination. International cooperation cannot compensate for fragmented governance at the national level.

From a legal policy perspective, the persistence of institutional fragmentation illustrates that Indonesian banking law continues to emphasize institutional authority rather than institutional integration. Existing legislation clearly distributes supervisory responsibilities among various public institutions, yet relatively limited attention has been devoted to establishing legally binding mechanisms governing collaborative governance, integrated supervision, joint strategic risk assessment, shared technological infrastructure, and synchronized institutional accountability. Consequently, institutional coordination frequently depends upon administrative cooperation or memoranda of understanding rather than upon comprehensive statutory obligations requiring continuous operational integration.

These institutional limitations demonstrate that the future of banking crime enforcement should no longer focus exclusively upon strengthening individual institutions through expanded legal authority. Rather, greater emphasis should be placed upon reconstructing the institutional architecture governing financial crime prevention itself. Strengthening OJK without improving financial intelligence coordination will produce incomplete supervision. Similarly, enhancing PPATK's analytical capability without strengthening prudential supervision will reduce the preventive value of financial intelligence. Effective financial crime governance therefore requires an integrated institutional model in which supervision, intelligence, investigation, prosecution, and asset recovery operate as interconnected components of a single regulatory ecosystem.

Accordingly, this study argues that Indonesia's legal framework should gradually evolve from a fragmented supervisory structure toward an Integrated Financial Crime Enforcement System, where OJK, PPATK, Bank Indonesia, the National Police, the Attorney General's Office, the Corruption Eradication Commission (KPK), and other competent authorities function within a coordinated governance network supported by real-time information exchange, harmonized regulatory standards, joint risk assessment, interoperable technological infrastructure, and collaborative institutional accountability. Such an approach would significantly enhance the capacity of Indonesian law enforcement institutions to identify, prevent, investigate, and recover assets associated with increasingly sophisticated banking crimes while simultaneously strengthening public confidence in the national financial system.

E. Reconstructing Indonesia's Banking Crime Enforcement: Toward an Integrated Financial Crime Enforcement Model

The foregoing analysis demonstrates that Indonesia's current legal framework has established comprehensive institutional authorities for banking supervision and anti-money laundering. Nevertheless, the effectiveness of banking crime enforcement remains constrained by fragmented institutional governance rather than insufficient legal regulation. The principal challenge is therefore not the absence of supervisory institutions but the absence of an integrated institutional architecture capable of transforming regulatory supervision, financial intelligence, criminal investigation, and asset recovery into a continuous enforcement process. Consequently, strengthening banking crime enforcement requires legal reconstruction directed toward institutional integration instead of merely expanding the authority of individual agencies.

Contemporary banking crimes differ fundamentally from conventional criminal offences because they evolve dynamically alongside financial innovation. Criminal organizations increasingly exploit digital banking services, cross-border payment systems, virtual assets, trade-based transactions, and complex corporate structures to disguise illicit financial activities. Such sophisticated financial schemes cannot be effectively detected through isolated institutional supervision. Rather, they require continuous interaction between regulatory supervision and financial intelligence capable of identifying hidden financial risks before criminal proceeds become fully integrated into the legitimate financial system.

This study therefore proposes an Integrated Financial Crime Enforcement Model (IFCEM) as a normative framework for strengthening banking crime enforcement in Indonesia. The proposed model is based upon the principle that financial crime prevention should operate through interconnected institutional governance rather than sequential institutional intervention. Instead of allowing supervisory authorities to function independently, IFCEM integrates prudential supervision, financial intelligence, criminal investigation, prosecution, judicial proceedings, and asset recovery within a unified regulatory ecosystem emphasizing prevention, early detection, coordinated enforcement, and financial system resilience.

The first component of IFCEM consists of preventive prudential supervision, implemented primarily by OJK through continuous risk-based supervision of banking institutions. Prudential supervision extends beyond verifying formal compliance with banking regulations by incorporating enterprise risk management, governance evaluation, customer due diligence, cybersecurity resilience, operational risk assessment, beneficial ownership transparency, and compliance with Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) obligations. Within this model, prudential supervision constitutes the earliest institutional barrier against banking crimes because weaknesses in governance frequently precede financial misconduct.

The second component comprises real-time financial intelligence integration coordinated by PPATK. Rather than functioning merely as a recipient of Suspicious Transaction Reports, PPATK should operate as the national financial intelligence hub capable of continuously integrating transaction reports, beneficial ownership information, international financial transfers, digital payment data, and financial crime typologies into a comprehensive national financial intelligence database. Artificial intelligence-assisted financial analytics, machine learning-based anomaly detection, and integrated digital reporting systems should gradually become essential technological instruments supporting early identification of sophisticated financial crime networks. Consequently, financial intelligence becomes a preventive regulatory instrument instead of merely an investigative tool.

The third component concerns institutional interoperability among supervisory and law enforcement agencies. Effective banking crime enforcement requires OJK, PPATK, Bank Indonesia, the Indonesian National Police, the Attorney General's Office, the Corruption Eradication Commission (KPK), the Directorate General of Taxes, Customs and Excise, and other competent authorities to operate within an interoperable governance structure supported by legally mandated information-sharing mechanisms. Institutional interoperability should not rely exclusively upon administrative memoranda of understanding but instead be supported by statutory obligations requiring secure real-time information exchange, standardized reporting protocols, joint institutional risk assessment, and coordinated strategic planning.

Another essential component of IFCEM involves the establishment of Joint Financial Crime Task Forces responsible for addressing complex banking crimes involving multiple jurisdictions or regulatory sectors. Unlike conventional investigative teams established after criminal proceedings commence, Joint Financial Crime Task Forces would function proactively by combining banking supervisors, financial intelligence analysts, forensic accountants, cybercrime specialists, prosecutors, and investigators into multidisciplinary operational teams. Such institutional collaboration enables simultaneous administrative supervision, financial intelligence analysis, criminal investigation, digital forensic examination, and asset tracing before criminal proceeds disappear through international financial networks.

An equally significant element concerns asset recovery integration. Traditional criminal justice systems frequently prioritize criminal conviction while treating confiscation of illicit assets as a secondary objective. However, international anti-money laundering standards increasingly recognize asset recovery as the ultimate objective of financial crime enforcement because organized financial crimes are primarily economically motivated. Consequently, IFCEM emphasizes early financial tracing, provisional asset freezing, beneficial ownership identification, international mutual legal assistance, and non-conviction-based asset recovery where legally permissible. Recovering illicit financial assets not only compensates economic losses but also disrupts the financial incentives sustaining organized criminal enterprises.

From a governance perspective, IFCEM further incorporates continuous institutional evaluation through measurable performance indicators extending beyond administrative outputs. Institutional effectiveness should no longer be assessed according to the number of inspections conducted, suspicious transaction reports received, or administrative sanctions imposed. Instead, performance evaluation should include indicators such as the speed of financial intelligence dissemination, the quality of inter-agency cooperation, the effectiveness of early risk identification, successful disruption of criminal financial networks, asset recovery outcomes, and public confidence in financial institutions. Such indicators more accurately reflect the preventive objectives underlying contemporary financial governance.

Legal reconstruction should likewise address regulatory harmonization. Several Indonesian statutes governing banking, financial supervision, anti-money laundering, corruption eradication, taxation, electronic transactions, and cybercrime continue to operate through separate legislative frameworks despite addressing interconnected financial misconduct. IFCEM therefore recommends gradual harmonization of these legal regimes through coordinated legislative reform emphasizing institutional integration, consistent legal terminology, harmonized reporting obligations, and unified regulatory objectives. Legislative harmonization would substantially reduce legal uncertainty while minimizing regulatory arbitrage exploited by sophisticated financial criminals.

Technological modernization represents another indispensable element of the proposed framework. Digital banking, blockchain technology, virtual assets, open banking, financial technology platforms, and decentralized finance increasingly generate enormous volumes of financial data exceeding the analytical capacity of conventional supervisory methods. Consequently, Indonesia should progressively integrate artificial intelligence, big data analytics, blockchain forensic technology, predictive financial risk analysis, and secure digital information exchange into its financial crime governance architecture. These technological innovations would significantly enhance institutional capacity to identify suspicious financial behavior in real time while reducing dependence upon reactive criminal investigations.

The proposed Integrated Financial Crime Enforcement Model ultimately reflects a paradigm shift from institution-centered regulation toward ecosystem-based financial governance. Rather than perceiving OJK and PPATK as separate public institutions exercising isolated legal mandates, the model conceptualizes financial supervision and financial intelligence as mutually reinforcing components of a unified national financial integrity system. Banking crime prevention therefore becomes a continuous governance process beginning with prudential supervision, strengthened through financial intelligence, coordinated through institutional collaboration, enforced through criminal justice mechanisms, and concluded through effective recovery of criminal assets.

Accordingly, this study argues that the future development of Indonesian banking law should prioritize institutional integration over institutional expansion. Expanding the legal authority of individual institutions without improving collaborative governance will merely reproduce existing regulatory fragmentation. By contrast, constructing an integrated institutional ecosystem supported by harmonized legislation, interoperable technology, real-time intelligence sharing, and collaborative law enforcement offers a substantially more sustainable strategy for safeguarding financial stability and combating increasingly sophisticated banking crimes in Indonesia.

IV. CONCLUSION AND SUGGESTIONS

A. Conclusion

This study demonstrates that the increasing complexity of banking crimes in Indonesia has fundamentally transformed the paradigm of financial crime enforcement from a reactive criminal justice approach toward an integrated preventive governance model. Banking crimes are no longer confined to conventional offences such as unauthorized banking activities, banking secrecy violations, or accounting manipulation as regulated under the Indonesian Banking Law. Instead, they have evolved into sophisticated financial crimes involving cyber-enabled fraud, cross-border money laundering, beneficial ownership concealment, digital financial transactions, and other forms of illicit financial flows that transcend the jurisdiction and institutional capacity of any single regulatory authority.

The findings indicate that the effectiveness of banking crime enforcement depends less upon the existence of comprehensive legislation than upon the degree of institutional coordination between prudential supervision and financial intelligence. OJK performs a strategic preventive function through risk-based banking supervision, governance assessment, regulatory compliance monitoring, and institutional risk management, whereas PPATK serves as Indonesia's Financial Intelligence Unit by transforming financial transaction reports into actionable intelligence supporting criminal investigations, asset tracing, and financial crime prevention. Although both institutions possess complementary legal mandates, the study identifies persistent challenges arising from fragmented institutional governance, overlapping regulatory responsibilities, delayed information exchange, and limited integration between administrative supervision and criminal law enforcement. These institutional weaknesses reduce the effectiveness of early detection, coordinated investigation, and recovery of criminal assets.

The principal contribution of this research lies in the development of the Integrated Financial Crime Enforcement Model (IFCEM) as a conceptual framework for strengthening Indonesia's banking crime enforcement system. Unlike existing approaches that emphasize institutional authority independently, IFCEM integrates prudential supervision, financial intelligence, criminal investigation, prosecution, judicial proceedings, and asset recovery within a collaborative governance structure supported by real-time information exchange, harmonized regulatory standards, technological interoperability, and joint institutional accountability. The proposed model repositions banking crime enforcement as a continuous governance process rather than a sequence of isolated institutional interventions.

Accordingly, this study argues that future legal reform in Indonesia should prioritize institutional integration rather than merely expanding the legal authority of individual agencies. Sustainable banking crime prevention requires the construction of an integrated financial governance ecosystem capable of combining regulatory supervision, intelligence-led enforcement, technological innovation, and collaborative institutional coordination. Such an approach would not only enhance the effectiveness of banking crime prevention but also strengthen public confidence, financial system integrity, and Indonesia's compliance with international standards governing anti-money laundering and financial crime governance

B. Suggestion

Based on the findings of this study, Indonesia should undertake comprehensive legal and institutional reforms aimed at strengthening integrated financial crime governance. First, legislative harmonization should be pursued to improve the coherence of banking regulation, anti-money laundering legislation, financial sector supervision, cybercrime regulation, and asset recovery mechanisms so that institutional coordination operates upon a unified legal foundation rather than fragmented statutory mandates.

Second, OJK and PPATK should establish a legally binding framework for real-time institutional information sharing supported by interoperable digital infrastructure, standardized reporting mechanisms, and integrated financial intelligence platforms capable of facilitating early detection of suspicious financial activities before substantial financial losses occur.

Third, the Government should institutionalize Joint Financial Crime Task Forces involving OJK, PPATK, Bank Indonesia, the Indonesian National Police, the Attorney General's Office, the Corruption Eradication Commission (KPK), the Directorate General of Taxes, Customs and Excise, and other relevant authorities. Such multidisciplinary cooperation would significantly strengthen preventive supervision, financial intelligence analysis, criminal investigation, and asset recovery within a coordinated governance framework.

Finally, Indonesia should progressively adopt international best practices promoted by the Financial Action Task Force (FATF), the Basel Committee on Banking Supervision (BCBS), the Egmont Group, and other international financial regulatory institutions by integrating artificial intelligence, big data analytics, blockchain forensic technology, beneficial ownership transparency, and intelligence-led supervision into its national banking regulatory system. Through these reforms, Indonesia will be better positioned to address increasingly sophisticated banking crimes while enhancing financial system resilience and reinforcing its credibility within the global financial community.

REFERENCE LISTAN

Alldridge, P. (2008). Money laundering and global financial regulation. *Journal of Law and Society, 35*(4), 437–463.

Basel Committee on Banking Supervision. (2024). *Core Principles for Effective Banking Supervision*. Bank for International Settlements.

Bantekas, I. (2003). The international law of money laundering. *American Journal of Comparative Law, 51*(2), 315–347.

John C. Coffee Jr.. (2006). *Gatekeepers: The Professions and Corporate Governance*. Oxford University Press.

Egmont Group. (2023). *Egmont Group Annual Report 2023*. Egmont Group Secretariat.

Financial Action Task Force. (2021). *Guidance on Digital Identity*. FATF.

Financial Action Task Force. (2022). *Guidance on Beneficial Ownership for Legal Persons*. FATF.

Financial Action Task Force. (2023). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations).* FATF.

Ferwerda, J. (2018). The economics of crime and money laundering. *Review of Law & Economics, 14*(3), 1–24.

Gilmore, W. C. (2011). *Dirty Money: The Evolution of International Measures to Counter Money Laundering and the Financing of Terrorism* (4th ed.). Council of Europe Publishing.

Greenberg, T. S., Gray, L., Schantz, D., Gardner, C., & Latham, M. (2009). *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*. World Bank.

International Monetary Fund. (2023). *Financial Sector Assessment Program*. International Monetary Fund.

Indonesia. (1998). *Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking*.

Indonesia. (2010). *Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering*.

Indonesia. (2011). *Law Number 21 of 2011 concerning the Financial Services Authority*.

Indonesia. (2019). *Financial Services Authority Regulation Number 38/POJK.03/2019 concerning Risk Management for Commercial Banks*.

Indonesia. (2021). *Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks*.

Indonesia. (2023). *Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector*.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*, 289–375.

Masciandaro, D. (2007). Financial intelligence units: Theory and practice. *Journal of Money Laundering Control, 10*(2), 104–115.

Nance, M. T. (2018). Financial intelligence and global security. *International Affairs, 94*(6), 1245–1263.

Nelson, N. (2017). *Memahami dan Menghindari Tindak Pidana Perbankan*. Otoritas Jasa Keuangan.

Organisation for Economic Co-operation and Development. (2023). *Global Anti-Corruption & Integrity Outlook*. OECD Publishing.

Pieth, M. (2016). International anti-money laundering standards. *European Journal of Crime, Criminal Law and Criminal Justice, 24*(2), 115–132.

Rawlings, G., & Sharman, J. C. (2019). National responses to transnational financial crime. *Regulation & Governance, 13*(1), 65–84.

Ryder, N. (2015). *Financial Crime in the 21st Century: Law and Policy*. Edward Elgar Publishing.

Ryder, N. (2018). *The Financial War on Terror*. Routledge.

Ryder, N. (2020). *White Collar Crime and Risk: Financial Crime, Corruption and the Financial Crisis*. Palgrave Macmillan.

Sharman, J. C. (2010). Shopping for anonymous shell companies. *Journal of Economic Perspectives, 24*(4), 127–140.

Simamora, D., Mulyadi, M., Marlina, M., & Siregar, M. (2022). Peranan Otoritas Jasa Keuangan dalam pemberantasan tindak pidana pencucian uang yang menggunakan bank sebagai instrumen kejahatan. *Locus: Jurnal Konsep Ilmu Hukum, 2*(1), 1–11.

Tsingou, E. (2010). Regulatory reactions to the global credit crisis. *Journal of International Banking Regulation, 11*(2), 118–130.

Unger, B., & Ferwerda, J. (2011). Money laundering in the real world. *Review of Law & Economics, 7*(3), 665–693.

United Nations Office on Drugs and Crime. (2022). *World Drug Report 2022*. United Nations Office on Drugs and Crime.

World Bank. (2022). *Enhancing Government Effectiveness and Transparency: The Fight Against Corruption*. World Bank.