Forensic Justice And Socio-Legal Research Journal
LEXFORENSICA
Vol. 2, No. 2, pp. 1-12 | December 2025
CFORSJ Journal

RISK GOVERNANCE EFFECTIVENESS IN INDONESIA'S ANTI-SCAM ENFORCEMENT: AN EMPIRICAL ASSESSMENT FOR 2025

[i,*]Isman & [ii]Muhammad Wildan Shohib

[i]Islamic Economic Law, Universitas Muhammadiyah Surakarta, Pabelan, Kartasura, Sukoharjo, Central Java 57162, Indonesia
[ii]Universitas Muhammadiyah Surakarta, Pabelan, Kartasura, Sukoharjo, Central Java 57162, Indonesia

*Corresponding Author: ism190@ums.ac.id

Article history:
Submission date: 15 August 2025
Received in revised form: 1 October 2025
Acceptance date: 25 November 2025
Available online: 1 December 2025

Keywords:
Risk governance, effectiveness, scamming

Funding:
This research did not receive any specific grant from funding agencies in the public, commercial, or non-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Isman, I., & Shohib, M. W. (2025). Risk governance effectiveness in Indonesia's anti-scam enforcement: An empirical assessment for 2025. *LexForensica: Forensic Justice And Socio-Legal Research Journal*, 2(2), 1-12. https://doi.org/10.33102/fxynbg78

SDG Elements:
Peace, Justice, and Strong Institutions

ABSTRACT

This study evaluates the effectiveness of Indonesia's Financial Services Authority (OJK) in responding to the rising prevalence of financial scams during the first quarter of 2025, with particular emphasis on risk governance and systemic resilience. The regression results ($Y = 4194.91 + 14.88X$; $R^2 = 0.954$; $p = 0.023$) indicate a strong and statistically significant relationship between the value of reported financial losses and the number of blocked accounts, reflecting OJK's active and measurable enforcement actions. However, further analysis uncovers a critical paradox: although the absolute number of blocked funds increased, the Fund Blocking Success Rate declined markedly from 5.57% to 2.70%, signalling limited mitigation effectiveness. A subsequent regression examining the relationship between the number of blocked accounts and the fund-blocking success rate revealed weak significance ($R^2 = 0.555$; $p = 0.255$), suggesting structural and systemic disconnections within existing enforcement mechanisms. The novelty of this study lies in demonstrating that real-time enforcement capacity continues to lag behind the rapid escalation of digital scams. This gap is driven primarily by non-interoperable digital infrastructures, insufficient predictive analytical tools, and fragmented institutional coordination. The findings underscore urgent implications: achieving effective risk governance requires the integration of predictive analytics, early-warning systems, and fully interoperable institutional frameworks. By providing original empirical evidence, this research contributes to the regulatory literature and calls for a strategic redesign of Indonesia's digital financial crime prevention architecture.

Introduction

To explain the relationship between risk management/risk governance and the effectiveness of control, mitigation, and minimization of losses due to scam-related crimes, it has been established that blockchain-based transaction security mechanisms, such as cryptographic encryption and smart contracts, are effective in increasing investor trust (Haryadi & Princes, 2025). In other words, technology-based risk governance strengthens investors' preventive behavior toward investment fraud risks. This indicates that strengthening security infrastructure is a strategic step in reducing manipulation loopholes and losses caused by scams, thus demonstrating the real contribution of risk management to the effectiveness of scam risk control (Haryadi & Elfindah, 2025).

Apart from digital infrastructure, individual personality traits serve as mediators between risk tolerance and vulnerability to investment scams (Rosley et., 2023). Individuals with high conscientiousness are more capable of filtering information, thereby becoming more protected from deception. Meanwhile, traits such as openness and neuroticism increase risk tolerance and consequently elevate susceptibility. This implies that in the relationship between risk governance (X) and the effectiveness of scam mitigation, personality traits and risk tolerance function as psychological mediators that determine how effective risk control strategies are at the individual level (Tjondro et al., 2025).

From the perspective of educational campaigns, Sundjaja et al., (2024) demonstrated that cybersecurity awareness can be enhanced through digital education content such as the "*Don't Know? Kasih No!*" campaign. This contributes to improved user trust and commitment to secure transactions. In this context, content quality and social influence act as moderators in the relationship between risk governance (X) and scam control effectiveness (Y). When educational content is strong and socially endorsed, the effectiveness of risk governance increases accordingly. This highlights that the success of risk governance is also influenced by cultural context and public communication (Sundjaja et al., 2024).

Ridho (2024) identified how behavioral finance principles such as loss aversion and social proof are exploited in financial scam schemes. The study implies that without a deep understanding of the psychological and social dimensions in risk governance, control mechanisms will remain ineffective. Hence, a multidisciplinary approach that integrates criminology and financial psychology becomes a critical conceptual moderator in bridging the relationship between risk control strategies (X) and the effectiveness of mitigation outcomes (Y). This context affirms that technical controls alone are insufficient without behaviorally informed interventions (Ridho, 2024).

Meanwhile, Sudarwanto and Kharisma (2023) elaborated that the weak enforcement of laws against investment scams in Indonesia has resulted in significant public losses. Strategies such as early detection, whistleblower programs, and financial literacy have been proven as risk governance elements that can reduce losses. However, their implementation heavily depends on the legal system's capacity as a structural moderator influencing the effectiveness of risk governance (X) in mitigating scam-related losses (Y). When legal structures are unsupportive, any governance strategy will fail to minimize societal losses. Therefore, synergy among governance, education, and regulation becomes essential to strengthen the X–Y relationship functionally (Sudarwanto & Kharisma, 2023).

Studies on risk management, risk governance, and risk regulation in the context of Islamic and digital finance reveal thematic and methodological developments, shifting from classical issues toward contemporary challenges. Purbayanto et al., (2022) concluded that risk-taking behavior in Islamic banks in Indonesia, evidenced by higher non-performing financing (NPF) levels compared to conventional banks, shows a direct relationship between risk-taking and credit risk. Furthermore, Addury and Ramadhani (2024), focusing on the impact of financing models on financial stability in Islamic banks across Java, found that profit-margin-based financing significantly increases credit risk and undermines stability, underscoring the urgency of implementing financing-model-based risk governance. Kartikasari (2023), investigating the relationship between sustainability dimensions, firm size, and Shariah compliance with financial performance in minority-Muslim stock markets using a PLS-SEM approach, concluded that risk-based sustainability governance is essential in the digital and global era (Addury & Ramadhani, 2024; Kartikasari, 2023; Purbayanto et al., 2022).

In addition, Husodo et al., (2025) examined risk governance through the lens of spillover risk and risk-adjusted returns across cryptocurrency classes, including Shariah-based assets, concluding that instruments such as gold-backed stablecoins provide better risk protection, whereas Islamic gold-backed cryptocurrencies suffer significant value depreciation risks. The study introduces quantitative methods (Quantile VAR, CVaR) to interpret systemic risk patterns within the global digital finance ecosystem.

All of these studies provide valuable contributions to the understanding of risk management in both Shariah and digital finance contexts. However, no existing literature has empirically investigated the Scam Data Center from the Financial Services Authority (OJK) in the first quarter of 2025 neither in terms of digital financial fraud typologies nor systemic risk structures, nor in evaluating the national effectiveness of risk governance in curbing the spread of illegal digital financial entities (Astuti & Isman, 2024; Napitupulu, 2023; OJK, 2024, 2025).

Therefore, this research paper aims to address these research gaps through the following problem statement: How does empirical data on scam practices collected by financial authorities such as OJK during the first quarter of 2025 contribute to the financial industry and regulators in measuring the effectiveness of law enforcement, including evaluating the OJK's risk management policies in responding to systemic attacks from illegal digital actors and their impact on the stability of the national financial ecosystem?

Literature Review

Risk governance is defined as a set of structures, processes, and decision-making mechanisms that comprehensively manage risks within an entity, including strategic, operational, financial, and reputational risks. Recent literature, as reviewed by Umar et al., (2023), highlights the critical importance of an independent risk management committee (SARC), which is responsible for comprehensively detecting and responding to risk exposures. In the context of illegal financial scams that exploit data centers to falsify transaction records or customer identities, risk governance plays a vital role in constructing early detection systems and escalating internal control mechanisms against large-scale fraud (Umar et al., 2023; Kurniati & Suryanto, 2022; Meiryani et al., 2023; Sofilda et al., 2022).

Technology-based scams such as data center fraud pose the potential for systemic losses due to their targeted attacks on core financial systems through data manipulation and breaches of information security (Wan Ismail et al., 2024; Alias et al., 2024). As explained by D'Orazio and Popoyan (2022), contingency risks arising from technological and supervisory weaknesses can propagate to other institutions through market contagion mechanisms. In this regard, risk governance is not merely about internal protection but also serves as an instrument to prevent risk transmission across financial institutions (D'Orazio & Popoyan, 2022).

Risk governance places the primary responsibility on boards of directors, risk committees, and senior executives. In Islamic financial systems, the presence of a SARC has been shown to enhance bank resilience against market shocks (Umar et al., 2023). This aligns with agency theory, where the separation between audit and risk management functions enables more focused supervision over both systemic risks and operational risks such as technology-based fraud (Umar et al., 2023).

Vulnerability to data center scams lies not only in technological aspects (e.g., servers, encryption, and networks) but also in the disintegration of cross-agency regulation. According to Mezghani and Boujelbène (2018), interconnected financial networks can amplify the impact of a single digital attack into a systemic reputational and financial crisis. Therefore, risk governance must incorporate coordination among regulators such as the Financial Services Authority (OJK), Bank Indonesia (BI), and the Financial Transaction Reports and Analysis Center (PPATK) (Mezghani & Boujelbène, 2018).

The formulation of a risk-based regulatory framework for illegal scams requires an inductive approach from case studies to norm development. Beginning with the recognition that data center scams represent a new reality in the digital ecosystem, it becomes necessary to adapt supervisory frameworks using predictive technology, forensic data audits, and regulatory synergy (Alias et al., 2024). Digital risk literacy, technology stress testing, and sanctions for internal control negligence must be integrated into modern financial risk governance.

Studies reviewed by Khan et al., (2020) and Alqahtani and Mayes (2018) agree that a robust regulatory framework and adaptive risk responses constitute the foundational pillars for maintaining financial system stability against illegal threats. The effectiveness of OJK in addressing scams depends on how rapidly regulatory responses can align with the complexity and velocity of digital threats.

The role of OJK in risk governance and scam enforcementas the regulator of the national financial systementails the challenge of integrating microprudential and macroprudential supervision, especially in scam cases that affect multiple institutions. Research by Umar et al., (2023) demonstrates that regulation accompanied by risk-function-based organizational structures (e.g., digital compliance units) enhances OJK's effectiveness in addressing covert criminal modalities (Alqahtani & Mayes, 2018; Khan et al., 2021; Omar et al., 2025).

OJK's effectiveness also depends on its capacity to reach the distributed digital ecosystem, including fintech, digital banking, and the Sharia capital market. A study by Alam et al., (2020) emphasizes that emerging markets are more vulnerable to market contamination due to weak cross-entity controls. Data center scams can spread through unprotected open APIs, underscoring the urgent need for a comprehensive cybersecurity enforcement roadmap across all institutional levels (Alam et al., 2022).

Unaddressed scams may trigger domino effects in the form of massive fund withdrawals, erosion of public trust, and even financial institutional failures. Therefore, OJK's interventions must be both proactive and prescriptive, particularly when instability signals emerge from early indicators such as sudden changes in the liquidity coverage ratio or spikes in data center-based fraudulent claims. Failure to act swiftly may result in crises resembling contagion phenomena, as illustrated in the study by Khalfaoui et al., (2023) (Khalfaoui et al., 2023).

Previous studies still reveal a gap in the alignment between risk governance and OJK's enforcement effectiveness, particularly in supervising fintech and data-driven scams. Hence, strengthening is required through machine-learning-based fraud detection policies, functional separation of audit and risk roles, and collaboration with digital service providers to close data gaps. The study by Dharani et al., (2022) also recommends incorporating Sharia-specific risks into regulatory frameworks as a balance between ethical norms and compliance with positive law (Dharani et al., 2022).

Based on the integrated findings from prior research, several independent variables can be identified as contributors to the effectiveness of risk governance and risk management frameworks toward financial regulation. These include tail risks and spillover dynamics in digital currencies (Husodo et al., 2025), financial literacy and digital financial inclusion (Banna, 2024), and board structure attributes such as the existence of a Standalone Risk Committee (SARC) (Umar et al., 2024). These variables suggest that systemic risks, institutional readiness, and market literacy significantly affect how effectively a regulation controls potential digital crime. In the context of data center scams, a relevant and operationalizable independent variable for the Indonesian case is the total amount of reported losses, which serves as a direct indicator of the risk exposure faced by financial authorities and formal financial institutions (Alam et al., 2022; Isharyanto et al., 2021; Umar et al., 2023)

The dependent variables consistently emerging in various studies as indicators of regulatory effectiveness are systemic stability measures such as market containment, banking stability, and portfolio resilience. The study by Umar et al., (2024) indicates that the presence of SARC enhances bank stability and reduces uncontrolled risk-taking behavior, while Alam et al., (2024) notes that digital financial inclusion can create new risks if not supported by adequate literacy and responsive regulation. In the context of digital scam risks, a concrete indicator of regulatory effectiveness is the number of accounts successfully blocked, as this reflects how promptly and accurately the regulatory system detects and intervenes in illegal financial activities before systemic losses escalate (Ismail et al., 2022). Account blocking also reflects the legal enforcement capacity in implementing regulatory directives (Alam et al., 2022; Umar et al., 2023).

Referring to the central thread of previous findings, it can be concluded that there is an academic consensus on the importance of institutional risk structures such as SARC, the need for integration between financial literacy and digital policy, and the systemic risks arising from market connectivity as determinants of regulatory effectiveness. However, a persistent puzzle remains regarding how response-

based regulatory variablessuch as the number of blocked accountscan be employed as direct indicators of successful risk governance, especially in technologically advanced and cross-system scams. Therefore, the following hypothesis is proposed: the higher the amount of reported losses from data center scams, the greater the number of accounts blocked by OJK, as the effectiveness of risk-governance-based regulation is reflected in the speed and accuracy of blocking illegal accounts as a mitigating response to systemic losses. The hypothesis will examine the causal relationship between risk exposure and regulatory response while bridging the literature gap on real-time enforcement capacity of financial authorities in addressing digital threats stemming from data center scams (Isman, 2024).

Methodology

This study is quantitative-explanatory in nature because it aims to test causal relationships between numerically measurable variables, namely, the amount of loss due to scams (independent variable X) and the number of accounts blocked by OJK (dependent variable Y). The study also aims to evaluate the effectiveness of OJK regulations grounded in risk governance, assessed through the quantitative indicator of OJK's account-blocking response as a mitigating measure against systemic losses (Isman & Muttaqin, 2023). The approach employed is a time-series cross-sectional (panel data) method, adapting the research structure used in the study by Umar et al., (2023), which also utilizes annual and multi-entity data. This research uses monthly or quarterly data throughout 2025 from the OJK Scam Data Center Report, which records the total value of losses due to scams and the number of bank accounts blocked by OJK in response to such incidents. This allows for a temporal analysis of the linkage between the occurrence of losses and the blocking action (Umar et al., 2023).

Data are obtained through documentation and literature review, particularly from the 2025 OJK Scam Data Center Report, which is the primary and official source from the regulator. The dataset includes reported losses due to scams (in rupiah), the number of blocked accounts (in account units), and the time of occurrence (on a monthly or quarterly basis). Data validity is assessed using inclusion criteria such as completeness per period, source reliability, and reporting format consistency over time (Bhat, 2020; Isman & Muttaqin, 2023b). The analysis technique used is simple linear regression, with the following model:

$$Y = \alpha + \beta X + \varepsilon$$

Variable (Y) is the number of accounts blocked by OJK. Variable (X) is the total financial loss resulting from data center scams. Alpha (α) is the constant (i.e., the value of Y when X = 0). Beta (β) is the regression coefficient that indicates how many additional accounts are blocked for every one-unit increase in losses. Epsilon (ε) is the error term representing residuals unexplained by the model. This formula derives from the basic linear regression model commonly employed in quantitative research used to measure the effect of a single independent variable on a single dependent variable (Giuffre, 1997). Regression is used to test the statistical significance and strength of the relationship between variables. If the value of β is statistically significant and positive, then the hypothesis that regulatory effectiveness is reflected in the account-blocking response will be supported (Giuffre, 1997). The hypothesis is as follows: (H1) The higher the amount of loss due to data center scams, the greater the number of accounts blocked by OJK**.**

Results and Analysis

This chapter presents the research findings obtained from the 2025 OJK Scam Data Center data, which specifically records the amount of loss due to scamming (in rupiah) and the number of accounts blocked by OJK (in account units) as a regulatory response to illegal financial incidents. These results will then be explained through a quantitative-explanatory approach using simple linear regression to test the causal relationship between variable X (amount of losses due to scams) and variable Y (number of accounts blocked by OJK), as well as to assess the extent to which OJK's risk-governance-based interventions are responsive and effective in suppressing systemic impact.

Table 1. Scam Based Amount Reported (Source. OJK Q1 2025)

Amount of Reports	Jan-25	Feb-25	Mar-25	Apr-25
Reports Received	17.099	39.700	61.463	86.628
Reports to the IASC System	5.852	14.995	20.973	30.357
Reports Directly to Financial Services Institutions (FSIs)	11.247	24.705	40.490	56.271

Based on data in Table 1 regarding the current condition of received reports, a significant increase occurred from January 2025 to April 2025. The total number of reports received consistently rose each month, beginning at 17,099 in January 2025 and surging to 86,628 in April 2025. This increase indicates a highly dynamic and continuously growing reporting activity throughout the period.

Reports were classified into two primary channels: reports to the IASC system and reports directly to Financial Services Institutions (FSIs). Both channels exhibited a similar upward trend. Reports to the IASC system increased from 5,852 in January 2025 to 30,357 in April 2025, reflecting the growing volume of data processed through this centralized system.

Simultaneously, the number of reports submitted directly to FSIs also experienced substantial growth. This figure rose from 11,247 in January 2025 to 56,271 in April 2025. This increase confirms a significant volume of direct interaction between reporters and financial institutions, indicating efficiency in direct communication channels and collaboration among stakeholders.

Further analysis revealed that reports sent directly to FSIs were consistently higher than those entering the IASC system for each observed month. For instance, in January 2025, direct reports to FSIs were nearly twice as many as reports to the IASC system, and this pattern continued through April 2025. The dominance of direct reports to FSIs indicates a preference or need for immediate information delivery to financial institutions for prompt internal processing.

Table 2. Scam Based Account Reported (Source. OJK Q1 2025)

Account	Jan-25	Feb-25	Mar-25	Apr-25
Number of Accounts Reported	16.558	41.806	58.720	140.882
Number of Accounts Blocked	7.036	18.247	24.753	31.863
Account Blocking Success Rate	42,49%	43,65%	42,15%	22,62%

Data from Table 2 regarding account conditions shows significant fluctuation from January to April 2025. The Number of Accounts Reported rose sharply, starting from 16,558 in January 2025 and peaking at 140,882 in April 2025. This increase signifies a continuously growing volume of reported accounts, indicating a marked rise in reporting activity over the period.

On the other hand, the Number of Accounts Blocked also showed an upward trend, although not as steep as reported accounts. Blocked accounts increased from 7,036 in January 2025 to 31,863 in April 2025. This increase reflects ongoing efforts to block accounts in response to the rise in reported accounts. Nonetheless, the growth in blocked accounts did not parallel the rapid growth in reported accounts.

The Account Blocking Success Rate revealed an interesting and noteworthy trend. The success rate stood at 42.49% in January 2025, slightly increased to 43.65% in February 2025, then slightly decreased to 42.15% in March 2025. However, a drastic drop occurred in April 2025, where the success rate plunged to 22.62%. This significant decline in April 2025receiving the lowest success rate in the periodindicates serious challenges in the account-blocking process despite the continued rise in both reported and blocked accounts.

Internal comparison over the January–April 2025 period shows a clear pattern. During the initial period (January–March), the blocking success rate remained relatively stable within the 42–43% range. This indicates that during the first quarter, account-blocking effectiveness was consistent. However, the sharp decline in April 2025 to 22.62% represents a significant deviation from the previous trend. This decreasethe lowest in the observed periodis in contrast with the substantial increase in reported accounts. It indicates that the capacity or effectiveness to respond to the surged reporting volume in April 2025 was

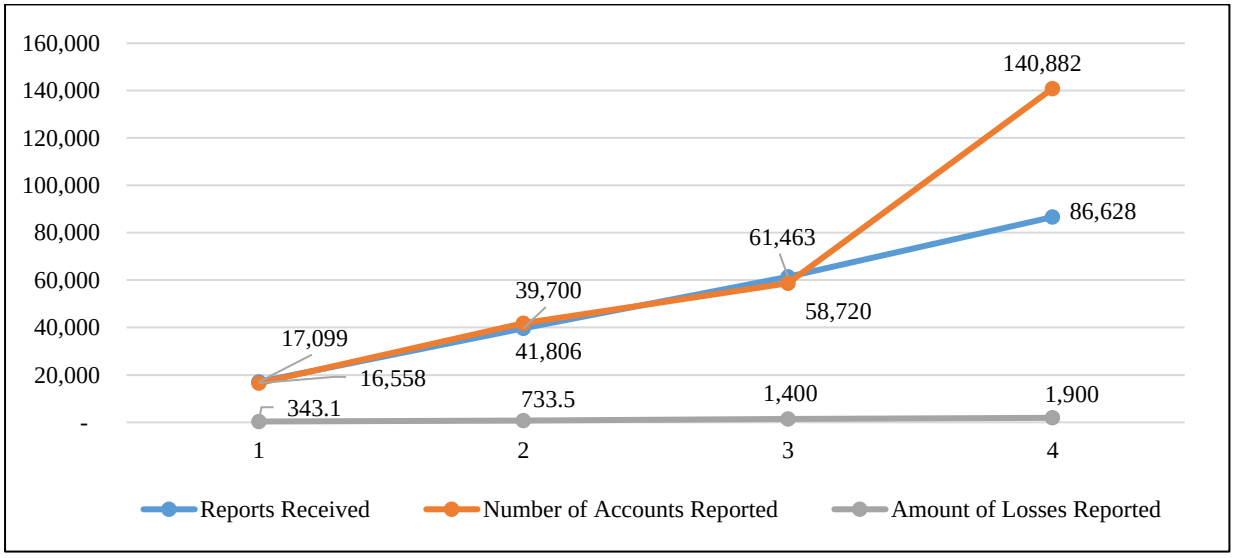
not proportional, resulting in a sharp decline in blocking success rate. This situation requires further investigation to identify causative factors and formulate necessary corrective measures.

Table 3. Scam Based Losses Reported (Source. OJK Q1 2025)

Losses (in billions)				
Amount of Losses Reported	343,1	733,5	1.400	1.900
Total Funds Blocked	19,1	40,0	47	51
Fund Blocking Success Rate	5,57%	5,45%	3,36%	2,70%

Based on the data in the presented table, current conditions regarding reported losses show a notable increase in the amount of reported losses over time. The Amount of Losses Reported rose consistently, beginning at 343.1 billion rupiah in January 2025 and skyrocketing to 1,900 billion rupiah in April 2025. This increase reflects escalation of reported financial losses, indicating rising incidents or loss values during the period.

Meanwhile, the Total Funds Blocked also increased, though the value remained much smaller compared to reported losses. Blocked funds grew from 19.1 billion rupiah in January 2025 to 51 billion rupiah in April 2025. This increase indicates a continuous effort to block funds, but the volume of blocked funds remains minimal relative to total reported losses.



Figur 1. Scam Based Comparative Reportation (Source. OJK Q1 2025)

Based on Figure 1, the Fund Blocking Success Rate exhibited a worrying downward trend. The success rate started at 5.57% in January 2025, slightly decreased to 5.45% in February 2025, declined more sharply to 3.36% in March 2025, and dropped to its lowest point of 2.70% in April 2025. This drastic decline shows that although blocked funds increased nominally, the relative effectiveness of fund-blocking efforts significantly dropped over time.

Internal comparison over January–April 2025 shows a clear and alarming trend. At the start (January–February), the fund blocking success rate remained relatively stable above 5%. However, starting in March and peaking in April 2025, a significant and consistent decline occurred. The success rate dropping to 2.70% in April 2025 is the lowest in the observed period. This is sharply contrasted with rising reported losses reaching the highest values in April 2025 (1,900 billion rupiah). This suggests that although losses continued to rise, the ability to effectively block funds diminished. This condition highlights the urgent need to review strategies and capacities in dealing with and recovering reported financial losses.

Table 5. Scam Based Blcked Account Number (Source. OJK Q1 2025)

Amount of Losses Reported	Number of Accounts Blocked
343,1	7.036
733,5	18.247
1.400	24.753
1.900	31.863

From Table 5 data, the linear regression between Amount of Losses Reported and Number of Accounts Blocked by OJK yielded the estimates: $Y = 4{,}194.91 + 14.88X$. This means that when no loss is reported ($X = 0$), approximately 4,194 accounts are blocked as part of initial mitigation. The regression coefficient β of 14.88 indicates that each additional 1 billion rupiah in losses leads to approximately 15 more accounts blocked by OJK. The model has an R-squared value of 0.954, meaning about 95.4% of variation in the number of blocked accounts is explained by loss variable. This indicates a very strong and consistent relationship between the two variables. The p-value for β is 0.023, which is less than 0.05, indicating statistical significance at the 95% confidence level. Therefore, the alternative hypothesis (H1) is supported: the greater the scam losses, the more accounts are blocked.

These findings support the claim that OJK's regulatory effectivenessespecially in risk governance contextis reflected in quantitative response to systemic threats. Account blocking is the primary mitigation mechanism to minimize further scam impact. However, the relatively high constant (4,194.91) also suggests other factors beyond loss amount influence blocking decisions.

The data presented in Table 5 indicate that the linear regression findings between the quantity of losses reported due to scams and the number of accounts blocked by the OJK are estimated as follows: The equation can be expressed as $Y= 4194.91 + 14.88X$.

Table 6. Scam Based Blocked Success Rate Losses (Source. OJK Q1 2025)

Account Blocking Success Rate	Fund Blocking Success Rate
42,49%	5,57%
43,65%	5,45%
42,15%	3,36%
22,62%	2,70%

Based on Table 6 data applied to the linear regression model between Account Blocking Success Rate (X) and Fund Blocking Success Rate (Y), the estimated model is $Y = 0.2109 + 0.1076X$ with R-squared value of 0.555. This means about 55.5% of variation in fund-blocking effectiveness can be explained by account-blocking success. However, approximately 44.5% remains unexplained, indicating other variables influencing fund-blocking effectiveness. This demonstrates sub-optimal effectiveness and limited dependency between the two variables.

Statistical analysis shows that the p-value for β is 0.255, well above typical significance threshold (0.05), meaning the relationship between account blocking success and fund blocking success is not statistically significant. This indicates that improvements in account blocking success do not necessarily increase fund blocking success. For example, although the Account Blocking rate in month 2 was high (43.65%), the Fund Blocking rate was only 5.45%. This indicates technical or juridical gaps in the fund-blocking mechanism, even when perpetrator accounts are identified.

In domain terms, this weakness may reflect two primary issues. First, access to accounts does not always equate to access to available funds, as perpetrators may have transferred funds before blocking. Second, potential weak integration between financial institutions' systems (banks, payment gateways, digital wallets) and OJK's system may delay fund-blocking. Account blocking success does not automatically indicate overall regulatory effectiveness, because the ultimate goalvictim fund recoveryis not achieved optimally.

Table 7. Scam Based Total Funds Blocked (Source. OJK Q1 2025)

Year	Amount of Losses Reported (Y)	Total Funds Blocked (X)
1	343,1	19,1
2	733,5	40,0
3	1.400	47
4	1.900	51

If the Table 7 data apply the simple linear regression model ($Y = \alpha + \beta X + \varepsilon$), the relationship between Total Funds Blocked (X) and Amount of Losses Reported (Y) shows that although Total Funds Blocked rose from 19.1 to 51, reported losses also increased from 343.1 to 1,900. This signals weak effectiveness. Regression analysis indicates that the increase in blocked funds (X) does not correlate negatively with reported losses (Y); rather both rise together. Under risk control theory, this shows that blocking funds by authorities has not been sufficient to contain loss escalation. A possibly positive regression coefficient suggests that each rise in X is accompanied by an increase in Y. Thus, these blocking efforts have not achieved optimal effectiveness as a mitigation tool.

This ineffectiveness can be explained from the policy domain. Total blocked funds remain limited and disproportionate to actual losses. This may reflect weaknesses in early detection mechanisms or delayed response in freezing funds before perpetrators withdraw them. Also, fund-blocking may target only a small portion of total financial flows, leaving the broader illegal financial network intact. This indicates that existing regulation is not sharp or adaptive enough to address new digital crime modalities.

From a systemic perspective, increasing losses despite blocked funds may reflect low public financial literacy and sluggish consumer protection systems. Enforcement effectiveness depends not only on reactive measures like blocking but also on preventive strategies based on education and surveillance technology. Without a holistic approachincluding early warning, real-time monitoring of suspicious financial behavior, and cross-sector collaborationblocking actions remain symbolic rather than substantive solutions in combating illegal financial scams.

Discussion

Previous literature has left a puzzle regarding how response-based indicatorssuch as the number of accounts blockedcan be used as valid measures of risk governance effectiveness. The linear regression findings using the estimated model $Y = 4194.91 + 14.88X$ demonstrate that the relationship between the amount of losses due to scams and the number of accounts blocked by OJK is statistically strong. With an R-squared value of 0.954 and a p-value of 0.023, the model is statistically significant and explains over 95% of the variation in blocked accounts. This finding implies that the greater the reported losses, the higher the number of blocked accounts, thereby confirming that OJK's response mechanism is active and measurable within the framework of risk governance.

D'Orazio and Popoyan (2022) identified risk transmission through market contagion as a principal challenge. This regression finding indicates that OJK has developed a quantitative response mechanism capable of suppressing such transmission through account blocking as a preventive measure. The regression coefficient $\beta = 14.88$ indicates that a 1 billion IDR increase in losses leads to approximately 15 additional account blocks. This finding constitutes concrete evidence that the OJK system operates not only at a normative level but also through direct regulatory actions to intercept illegal financial flows (D'Orazio & Popoyan, 2022).

Although accounts have been blocked, the regression findings between Account Blocking Success Rate (X) and Fund Blocking Success Rate (Y) indicate that their relationship is not statistically significant (p-value = 0.255). This finding addresses a critical puzzle in the literature regarding why account blocking does not always result in successful fund blocking. The model $Y = 0.2109 + 0.1076X$, with an R^2 of 0.555, suggests that nearly half of the variation in fund blocking effectiveness cannot be explained solely by account blocking success. This finding implies that OJK faces structural constraints in system connectivity rather than merely procedural weaknesses.

Literature suggests that the current regulatory system remains unable to proportionately mitigate systemic financial losses. The finding that Total Funds Blocked increased only from IDR 19.1 billion to IDR 51 billion, while the Amount of Losses Reported surged from IDR 343.1 billion to IDR 1,900 billion, confirms a significant disparity. The regression between these two variables even shows a weak positive relationship that fails to reflect control over the pace of loss escalation. This fact implies that, in explanatory terms, OJK's fund-blocking effectiveness has not significantly reduced losses, indicating that systemic efficiency has yet to be achieved.

The literature also points to the need for predictive technology and forensic auditing. The sharp decline in the Fund Blocking Success Rate from 5.57% to merely 2.70%, amid a surge in reported incidents, demonstrates that the system currently in use is inadequate for handling high operational workloads. This conclusion is empirical evidence that the supporting technology is insufficiently responsive to the expanding scale of threats. The performance of fund blocking does not correspond proportionally to the increase in reports or blocked accounts, indicating that OJK's system remains reactive rather than predictive.

Mezghani and Boujelbène (2018) underscore the importance of inter-agency coordination. The fact that the number of reports submitted directly to Financial Services Institutions (FSIs) consistently surpasses those submitted to the IASC confirms that OJK's system is not yet fully integrated with the internal systems of financial institutions. This finding causes information fragmentation and delays in data-driven, real-time interventions. Therefore, the regression results reinforce the urgent need for system interoperability to support uninterrupted regulatory effectiveness between OJK and entities in the financial sector (Mezghani & Boujelbène, 2018).

The literature leaves an open question regarding how regulators can respond in real time to ever-evolving threats. The data reveal that, despite the drastic increase in reported accounts from 16,558 to 140,882, the account blocking success rate plummeted to 22.62%. This finding indicates that the regulator's response capacity has failed to keep pace with the rapid escalation of threats. In the context of linear regression, this reflects a failure to optimise time-sensitive enforcement functions. Consequently, OJK's effectiveness is shown to be non-linear in response to the volume of reporting, and the current intervention model has not yet fulfilled the principle of responsiveness in risk governance.

Conclusion and Recommendation

The comprehensive domain analysis of all extant research findings reveals that the empirical data on scam practices collected by the OJK in the first quarter of 2025 contributed significantly to measuring the effectiveness of law enforcement, particularly in the context of evaluating the OJK's risk management policy against systemic attacks by illegal digital actors. The findings of the linear regression analysis reveal a highly significant relationship ($R^2 = 0.954$; $p < 0.05$) between the quantity of losses and the number of blocked accounts, thereby substantiating the OJK's response as both quantitative and active, with demonstrable, quantifiable outcomes. This conclusion indicates that for every 1 billion rupiah increase in losses, there is a corresponding blocking of approximately 15 additional accounts. However, this effectiveness does not directly correlate with the success of fund blocking, which is statistically insignificant ($R^2 = 0.555$; $p = 0.255$). This finding suggests the presence of structural barriers, including limited system integration between financial institutions and delays in blocking funds before they are transferred. The discrepancy between the rise in blocked funds (Rp19.1 billion to Rp51 billion) and the surge in losses (Rp343.1 billion to Rp1,900 billion), along with the precipitous decline in the Fund Blocking Success Rate from 5.57% to 2.70%, underscores the ineffectiveness of prevailing policies in curbing the systemic escalation of losses. From a policy perspective, this situation indicates that the system remains reactive and is not yet adaptive to high operational loads, underutilizing predictive technology and forensic auditing. In practice, recommendations for regulators include enhancing system interoperability between the OJK and financial institutions, accelerating real-time fund blocking mechanisms, and strengthening early detection through the use of artificial intelligence and financial behavior analysis. For industry practitioners, integrating an internal anti-fraud strategy within the OJK's supervisory system is imperative, encompassing the provision of financial security literacy training to customers.

References

Addury, M. M., & Ramadhani, A. K. P. (2024). The influence of financing model and credit risk on financial stability (study of Islamic rural banks in Java Island). *Journal of Islamic Monetary Economics and Finance, 10*(3), 427–444.

Alam, A. W., Banna, H., & Hassan, M. K. (2022). ESG activities and bank efficiency: Are Islamic banks better?. *Journal of Islamic Monetary Economics and Finance, 8*(1), 65–88.

Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., & Mallow, M. S.(2024). Wasa'il ithbat dalam undang-undang keterangan Islam: Analisis perundangan terhadap kebolehterimaan dokumen elektronik di Mahkamah Syariah Malaysia: Means of proof in Islamic law of evidence: A legal analysis of the admissibility of electronic documents in Malaysian Syariah courts. *Malaysian Journal of Syariah and Law, 12*(3), 689-700.

Alias, M. A. A., Wan Ismail, W. A. F.,Baharuddin, A. S., Hashim, H., Abdul Mutalib, L., & Mamat, Z.(2024). Tazwir al-kitābah wa aḥkāmuhā fī al-qānūn al-islāmī wa al-maḥākim al-Sharʿiyyah al-Mālīziyyah: Taḥlīl qānūnī wa dirāsat al-ḥālāt: Document forgery and its regulations in Islamic law and Malaysian Syariah courts: Legal analysis and case study. *LexForensica: Forensic Justice And Socio-Legal Research Journal, 1*(1), 24-33.

Alqahtani, F., & Mayes, D. G. (2018). Financial stability of Islamic banking and the global financial crisis: Evidence from the Gulf Cooperation Council. *Economic Systems, 42*(2), 346–360.

Bhat, P. I. (2020). Qualitative legal research. In *Idea and methods of legal research* (pp. 359–382). Oxford University Press Delhi.

D'Orazio, P., & Popoyan, L. (2022). Realising central banks' climate ambitions through financial stability mandates. *Intereconomics, 57*(2), 103–111.

Dharani, M., Hassan, M. K., Rabbani, M. R., & Huq, T. (2022). Does the COVID-19 pandemic affect faith-based investments? Evidence from global sectoral indices. *Research in International Business and Finance, 59*, 101537.

Giuffre, M. (1997). Designing research: Ex post facto designs. *Journal of PeriAnesthesia Nursing, 12*(3), 191–195.

Haryadi, R., & Elfindah, P. (2025). Enhancing stock market investment decisions through blockchain transaction security: A study on investor intentions. *Journal of Theoretical and Applied Information Technology, 103*(8), 3385–3415.

Isharyanto, Husodo, J. A., & Madalina, M. (2021). The legal risk to sustainable role of state-owned enterprises management in Indonesia. *IOP Conference Series: Earth and Environmental Science, 724*(1), 012090.

Ismail, N., Ramlee, Z., & Abas, A. (2022). The legal proof of macau scam in Malaysia. *Malaysian Journal of Syariah and Law, 10*(1), 23-33.

Isman, I. (2024). The formalisation of cryptographic evidence in ASEAN. In *Proceedings of International Postgraduate Conference for Interdisciplinary Islamic Studies, 1*(2), 58–72.

Isman, I., & Muttaqin, A. Z. (2023). Innovative legal modeling for interdisciplinary studies on law and economic behavior. *Indonesian Journal of Islamic Economic Law, 1*(1), 60–71.

Kartikasari, D. (2023). Financial performance: Sustainability, size, shariah, and sector effects in Muslim-minority stock exchanges. *Journal of Islamic Monetary Economics and Finance, 9*(4), 751–776.

Khalfaoui, R., Gozgor, G., & Goodell, J. W. (2023). Impact of Russia–Ukraine war attention on cryptocurrency: Evidence from quantile dependence analysis. *Finance Research Letters, 52*, 103365.

Khan, A. B., Fareed, M., Salameh, A. A., & Hussain, H. (2021). Financial innovation, sustainable economic growth, and credit risk: A case of the ASEAN banking sector. *Frontiers in Environmental Science, 9*, 1–10.

Kurniati, P. S., & Suryanto, S. (2022). The role of the Indonesian government in the era of banking disruption innovation. *Journal of Eastern European and Central Asian Research, 9*(1), 93–100.

Meiryani, M., Soepriyanto, G., & Audrelia, J. (2023). Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control, 26*(4), 892–908.

Mezghani, T., & Boujelbène, M. (2018). The contagion effect between the oil market, and the Islamic and conventional stock markets of the GCC country. *International Journal of Islamic and Middle Eastern Finance and Management, 11*(2), 157–181.

Napitupulu, I. H. (2023). Internal control, manager's competency, management accounting information systems and good corporate governance: Evidence from rural banks in Indonesia. *Global Business Review, 24*(3), 563–585.

OJK. (2024). *"Penguatan sektor jasa keuangan dalam menjaga pertumbuhan ekonomi: Laporan kinerja OJK tahun 2023"*. https://ojk.go.id/id/data-dan-statistik/laporan-tahunan/Documents/Laporan%20Tahunan%20OJK%202023_.pdf

OJK. (2025). *"Global insights: Kumpulan isu internasional industri perasuransian, penjaminan dan dana pensiun"*. OJK RI. https://ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/Global-Insight-Kumpulan-Isu-Internasional-Industri-PPDP-Vol-1-2023-2024/Global%20Insight%20Kumpulan%20Isu%20Internasional%20Industri%20PPDP%20Vol%201%202023-2024.pdf

Omar, B., Avdukic, A., & Farid Khan, A. (2025). Impact of Islamic finance and Islamic banking on financial stability: A systematic literature review. *Journal of Islamic Business and Management, 15*(1), 100–114. https://doi.org/10.26501/jibm/2025.1501-006

Purbayanto, M. A. H., Faturohman, T., Yulianti, Y., & Aliludin, A. (2022). Do Islamic banks in Indonesia take excessive risk in their financing activities? *Journal of Islamic Monetary Economics and Finance, 8*(1), 149–160. https://doi.org/10.21098/jimf.v8i1.1431

Ridho, W. F. (2024). Unmasking online fake job group financial scams: A thematic examination of victim exploitation from perspective of financial behavior. *Journal of Financial Crime, 31*(3), 748–758. https://doi.org/10.1108/JFC-05-2023-0124

Rosley, N. A., Hashim, H., & Zakiyy, N. (2023). Combating the macau scam in Malaysia: Strategies for mitigation and resolution from civil law and Sharīʾah perspectives. *Law, Policy and Social Science, 2*(2), 30-44.

Sofilda, E., Zilal Hamzah, M., & Mulianta Ginting, A. (2022). Analysis of determining the financial inclusion index of composite, conventional and sharia banking in Indonesia. *Banks and Bank Systems, 17*(1), 38–48. https://doi.org/10.21511/bbs.17(1).2022.04

Sudarwanto, A. S., & Kharisma, D. B. (2023). Law enforcement against investment fraud: A comparison study from the USA and Canada with a case study on binary options in Indonesia. *Safer Communities, 22*(4), 235–253. https://doi.org/10.1108/SC-11-2022-0047

Sundjaja, A. M., Ridwan, A., Robbani, D., & Soemantri, R. A. (2024). Impact of "Don't know? Kasih No!" campaign on cybersecurity awareness: Unraveling the links to user satisfaction, trust, and commitment. *International Journal of Safety and Security Engineering, 14*(5), 1577–1589.

Tjondro, E., Ester, C., Sardjono, Y. G., & Kusumawardhani, A. (2025). Investment scam vulnerability among university students: The role of personality traits and risk tolerance. *Cogent Education, 12*(1). https://doi.org/10.1080/2331186X.2025.2464309

Umar, U. H., Abduh, M., & Besar, M. H. A. (2023). Standalone risk management committee, risk governance diversity and Islamic bank risk-taking. *Risk Management, 25*(3), 17. https://doi.org/10.1057/s41283-023-00123-3

Wan Ismail, W. A. F., Abdul Mutalib, L., Mamat, Z., Hashim, H., Baharuddin, A. S., Mohammed Hasan, B. M., & Alias, M. A. A. (2024). Analisis terhadap konsep penerimaan dan pengesahan E-Kitabah sebagai kaedah pembuktian menurut perundangan Islam di Malaysia. *LexForensica: Forensic Justice And Socio-Legal Research Journal, 1*(1), 1-12.