



Legal Certainty for Digital Investors Through the Reconstruction of SupTech Based on Electronic System Reliability

Michael Lauvino^{1*}, Ismiyanto Ismiyanto², & Ariy Khaerudin³

^{1,2,3}Universitas Islam Batik
Surakarta, Indonesia

Correspondence

Michael Lauvino, Universitas Islam
Batik Surakarta, Indonesia, Jl. Agus
Salim No.10, Sondakan, Kec.
Laweyan, Kota Surakarta, Jawa
Tengah 57147, e-mail:
michael.lauvino@gmail.com

How to cite

Lauvino, Michael., Ismiyanto,
Ismiyanto., & Khaerudin, Ariy.
2026. Legal Certainty for Digital
Investors Through the
Reconstruction of SupTech Based
on Electronic System Reliability.
Jurnal Ilmu Hukum Kyadiren 8(1),
706-722.
<https://doi.org/10.46924/jihk.v8i1.494>

Original Article

Abstract

Digital transformation has significantly increased the number of retail investors in Indonesia while simultaneously amplifying the risk of financial losses resulting from failures in digital investment service systems. However, the existing legal framework has not yet established adequate standards for ensuring the reliability of electronic systems. This study aims to analyze the regulatory framework governing cybersecurity and the financial services sector in providing legal protection for retail investors and to formulate a supervisory reconstruction model for the Financial Services Authority through the adoption of Electronic-Based Government System (SPBE) principles as the foundation for the development of Supervisory Technology (SupTech). This research employs a normative legal method using statutory, conceptual, analytical, and comparative approaches. The findings reveal regulatory gaps concerning electronic system reliability standards, parameters for determining system failures, and the allocation of liability among digital investment service providers. This study proposes a SupTech-based supervisory model that strengthens legal certainty, enhances preventive legal protection for retail investors, and promotes more accountable, transparent, and resilient digital investment governance.

Keywords: *Legal Protection, Retail Investors, Electronic-Based Government System (SPBE), Digital Investment*

Abstrak

Perkembangan digital telah meningkatkan jumlah investor ritel di Indonesia, tetapi juga memperbesar risiko kerugian akibat kegagalan sistem layanan investasi digital yang belum didukung standar hukum mengenai keandalan sistem elektronik. Kajian ini bertujuan menganalisis kerangka regulasi siber dan sektor jasa keuangan dalam melindungi investor ritel serta merumuskan model rekonstruksi pengawasan Otoritas Jasa Keuangan melalui penerapan prinsip Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai dasar pengembangan Supervisory Technology (SupTech). Penelitian menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, analitis, dan komparatif. terdapat kekosongan norma mengenai standar keandalan sistem, parameter pembuktian kegagalan sistem, dan distribusi tanggung jawab penyelenggara. kajian ini menawarkan model pengawasan berbasis SupTech yang memperkuat kepastian hukum, meningkatkan perlindungan hukum preventif, serta mendorong tata kelola investasi digital yang lebih akuntabel.

Kata kunci: *Perlindungan, Investor Ritel, Sistem Pemerintahan, Investasi Digital*

1. INTRODUCTION

Digital transformation has fundamentally reshaped Indonesia's financial services industry, particularly the capital market sector. Advances in information technology have enabled investors to conduct the entire investment process online through smartphone-based applications, including opening securities accounts, purchasing mutual funds, trading stocks and bonds, and investing in various digital financial assets. The rapid growth of wealth technology (wealthtech) platforms has significantly expanded public access to investment services and strengthened financial inclusion nationwide. According to the Indonesian Central Securities Depository (KSEI), the number of Single Investor Identification (SID) accounts increased from approximately 1.6 million in 2018 to 12.16 million by the end of 2023, reaching approximately 14.8 million by the end of 2024. This substantial growth indicates that digital platforms have become the primary channel through which retail investors participate in Indonesia's capital market.

The widespread adoption of digital investment platforms has fundamentally altered the paradigm of investor protection. Traditional legal protection has primarily focused on issues such as information disclosure, insider trading, market manipulation, and contractual breaches. In the digital era, however, legal risks increasingly arise from investors' dependence on electronic systems that support investment services. Digital investment transactions rely on the seamless integration of multiple technological infrastructures, including data centers, cloud computing services, application programming interfaces (APIs), communication networks, payment systems, and custodian banking services.¹ Consequently, a failure in any component of this digital ecosystem may interrupt transaction processes and expose investors to substantial financial losses. Accordingly, the reliability of electronic systems has evolved from a purely technical concern into a fundamental legal issue involving legal certainty, consumer protection, and the liability of digital investment service providers.

Indonesia has established a legal framework requiring electronic system providers to ensure the reliability and security of their systems. Article 15 of Law No. 1 of 2024 on Electronic Information and Transactions requires every electronic system provider to operate a reliable, secure, and accountable electronic system. Nevertheless, the legislation does not specify operational standards regarding system reliability, minimum service availability, performance benchmarks, or acceptable disruption thresholds that could serve as objective criteria for determining legal liability. Moreover, standard contractual clauses commonly used by digital investment platforms frequently limit providers' liability for losses resulting from system failures, despite the possibility that

¹ Hui Jiang, "How Does Computing Infrastructure Deployment Drive Corporate Digital Technology Innovation?," *Finance Research Letters* 86 (2025): 108659, <https://doi.org/10.1016/j.frl.2025.108659>.

such limitations conflict with Article 18 of Law No. 8 of 1999 on Consumer Protection, which restricts unfair exclusion-of-liability clauses.

Recent regulatory reforms in the financial services sector, particularly Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (P2SK Law), have expanded the regulatory authority of the Financial Services Authority (OJK) to oversee technological innovation in financial services. At the same time, the Electronic-Based Government System (SPBE) framework has introduced governance principles emphasizing system reliability, cybersecurity, accountability, interoperability, and effective electronic governance. However, these principles have not yet been systematically integrated into OJK's supervisory framework as minimum reliability standards for digital investment platforms or as the regulatory foundation for the development of Supervisory Technology (SupTech). Consequently, investor protection remains predominantly reactive, providing remedies only after losses have occurred, while preventive supervision based on measurable technological reliability standards has yet to be effectively implemented.

The rapid digitalization of Indonesia's financial sector has fundamentally transformed investment behavior and significantly increased retail investor participation. The number of Single Investor Identification (SID) accounts grew from approximately 1.6 million in 2018 to more than 12 million by the end of 2023, reflecting the success of digital investment platforms in expanding financial inclusion and broadening public participation in the capital market. Despite these achievements, the legal framework governing digital investment services has not kept pace with technological developments. Existing regulations continue to exhibit significant normative gaps concerning electronic system reliability standards, the allocation of liability for system failures, and the implementation of technology-driven supervisory mechanisms. These shortcomings underscore the need for a more comprehensive regulatory framework capable of ensuring legal certainty and providing effective preventive legal protection for retail investors in Indonesia's increasingly digital investment ecosystem.

These developments have stimulated a growing body of scholarship on the legal protection of digital investors. Nevertheless, the existing literature has primarily focused on consumer protection, the legality of investment instruments, personal data protection, digital fraud, insider trading, and the enforcement of laws against illegal investment schemes. Comparatively little attention has been devoted to legal protection against investor losses arising from failures of electronic systems, despite the increasing dependence of digital investment transactions on information technology infrastructure and the corresponding growth of systemic technological risks.

Research on the legal protection of digital investors has expanded considerably but remains dominated by discussions of consumer rights, cybersecurity, digital fraud,

and regulatory compliance. Bari and Raodah argue that the legal relationship between investors and digital investment service providers is governed by multiple legal frameworks, including the Consumer Protection Law, the Investment Law, the Electronic Information and Transactions (ITE) Law, and regulations governing crypto assets. Their study emphasizes investor education, regulatory strengthening, effective supervision, and law enforcement but does not specifically examine the liability of service providers when investor losses result from failures of electronic systems.² Similarly, Yuniarti and Mahatma identify weak regulatory implementation, inadequate data security, digital fraud, and limited investor literacy as the principal challenges facing digital investment. However, their study does not formulate legal parameters for assessing electronic system reliability as a mechanism of preventive legal protection.³

Rahmat et al. distinguish between preventive and repressive forms of legal protection and highlight digital fraud as a significant threat to investors. However, their analysis does not address the technological standards that regulators should adopt to prevent losses resulting from operational failures of digital investment platforms.⁴ Likewise, Mukhlisin advocates the standardization of cybersecurity measures, blockchain technology, environmental, social, and governance (ESG) principles, and regulatory sandboxes. Nevertheless, the study primarily focuses on the development of the digital capital market ecosystem rather than establishing legal standards governing the liability of electronic system operators.⁵

At the international level, Lim underscores the importance of coordinated regulatory oversight among financial authorities but does not connect such coordination with technical standards for electronic system reliability.⁶ Ridwan demonstrates that the regulatory framework established under the P2SK Law and Financial Services Authority Regulation (POJK) No. 23 of 2025 has strengthened investor protection, although significant deficiencies remain regarding accountability standards for digital platforms and compensation mechanisms for losses caused by system failures.⁷ Meanwhile, studies by Maulana and Hariri, Mustovich et al., and Vijayaputro primarily examine insider trading, Islamic capital markets, and the security

² Abdulbari Bari and Putri Raodah, "Perlindungan Hukum Terhadap Investor Dalam Kegiatan Investasi Digital Di Indonesia," *Commerce Law* 4, no. 1 (2024): 61–69, <https://doi.org/10.29303/commercelaw.v4i1.4693>.

³ Erika Yuniarti and Bayu Mahatma, "Perlindungan Hukum Terhadap Investor Dalam Investasi Digital Di Indonesia: Analisis Kebijakan Dan Tantangan Regulasi Di Era Digital," *Simpul: Jurnal Ilmu Politik Dan Hukum* 1, no. 2 (2025): 30–36, <https://doi.org/10.71094/simpul.v1i2.128>.

⁴ Rahmat Rahmat et al., "Perlindungan Hukum Bagi Investor Ritel Dalam Transaksi Efek Di Pasar Modal Indonesia," *Jurnal Analisis Hukum Dan Kebijakan* 6, no. 2 (2025): 162–70.

⁵ Raden Muhammad Mukhlisin, "Transformasi Hukum Pasar Modal Di Era Digital: Pilar Investasi Dan Pembangunan Ekonomi," *Yustisi* 12, no. 3 (2025): 175–89, <https://doi.org/10.32832/yustisi.v12i3.19858>.

⁶ Feili Lim, "Perlindungan Hukum Bagi Investor Dalam Era Transformasi Digital: Kajian Hukum Bisnis Di Indonesia," *Media Hukum Indonesia* 3, no. 4 (2025): 93–97, <https://doi.org/10.5281/ZENODO.17263115>.

⁷ Mochammad Samsi Ridwan, "Perlindungan Hukum Investor Ritel Dalam Perdagangan Aset Keuangan Digital Pasca POJK Nomor 23 Tahun 2025," *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 4, no. 2 (2026): 1514–46, <https://doi.org/10.62976/ijjel.v4i2.1829>.

of non-fungible token (NFT) transactions. Collectively, these studies do not treat electronic system reliability as a central object of legal protection, thereby leaving an important research gap concerning legal standards for digital investment platform reliability as a foundation for provider liability and preventive investor protection.⁸

The existing literature generally examines the legal protection of digital investors from the perspectives of consumer protection, cybersecurity, law enforcement, insider trading, and digital investment regulation. However, no previous study has comprehensively integrated the Electronic Information and Transactions (ITE) Law, the Consumer Protection Law, the P2SK Law, and the Electronic-Based Government System (SPBE) framework to formulate a preventive supervisory model for ensuring the reliability of digital investment platforms. The principal contribution of the present study lies in its conceptual framework, which positions the SPBE principles of reliability not as obligations directly imposed upon private business entities but as normative benchmarks for the Financial Services Authority (OJK) in designing Supervisory Technology (SupTech) and developing technology-based supervisory standards. This approach aims to strengthen preventive oversight and enhance legal certainty before investor losses occur as a result of failures in electronic systems.

Against this background, the present study seeks to analyze the regulatory framework governing the legal protection of retail investors against losses arising from failures of digital investment service systems by examining the Electronic Information and Transactions (ITE) Law, the Consumer Protection Law, the P2SK Law, and relevant OJK regulations. Furthermore, the study proposes a model for reconstructing OJK's supervisory framework based on the principles of the Electronic-Based Government System (SPBE) to support the development of Supervisory Technology (SupTech). The proposed model is intended to strengthen electronic system reliability standards, enhance legal certainty, and provide more effective preventive legal protection for retail investors in Indonesia's rapidly evolving digital investment ecosystem.

2. RESEARCH METHODOLOGY

This study employs a normative legal research methodology to examine the legal norms governing the protection of retail investors against losses resulting from failures of electronic systems on digital investment platforms. This methodological approach was

⁸ Mohamad Rafi Maulana and Achmad Hariri, "Perlindungan Hukum Bagi Investor Ritel Terhadap Praktik Insider Trading Di Pasar Modal," *Jurnal Ilmiah Advokasi* 14, no. 1 (2026): 90–107, <https://doi.org/10.36987/jiad.v14i1.6995>; Munna Hidayatul Mustoviah et al., "Perlindungan Hukum Bagi Investor Ritel Dalam Perubahan Efek Syariah Pasca Pojk Nomor 8 Tahun 2025 Di Pasar Modal Syariah Indonesia," *Syariah: Jurnal Ilmu Hukum* 3, no. 4 (2026): 310–18, <https://doi.org/10.62017/syariah.v3i4.8560>; Muhammad Raditya Vijayaputro, "Perlindungan Hukum Mengenai Investasi Digital Dalam Bentuk Non-Fungible Token Berdasarkan Undang-Undang Nomor 25 Tahun 2007," *Unes Law Review* 6, no. 2 (2023): 4397–402, <https://doi.org/10.31933/unesrev.v6i2.1276>.

selected because the research addresses regulatory ambiguity and normative inconsistencies concerning electronic system reliability standards as the legal basis for determining the liability of digital investment service providers. The study adopts a statutory approach to analyze the interrelationship among the Electronic Information and Transactions (ITE) Law, the Consumer Protection Law, the Law on the Development and Strengthening of the Financial Sector (P2SK Law), the Capital Market Law, the Presidential Regulation on the Electronic-Based Government System (SPBE), and relevant Financial Services Authority (OJK) regulations governing information technology governance and consumer protection within the financial services sector.

In addition, the study applies a conceptual approach to examine the legal theories of legal protection, liability, information technology governance, electronic system reliability, and Supervisory Technology (SupTech). An analytical approach is further employed to interpret legal concepts that remain insufficiently defined within the existing regulatory framework. The research relies on primary, secondary, and tertiary legal materials collected through an extensive literature review. These legal materials are analyzed qualitatively using a prescriptive legal analysis method involving the identification of regulatory conflicts, normative gaps, and legal ambiguities. Based on this analysis, the study develops a process of legal harmonization and legal construction to formulate a supervisory model for the Financial Services Authority (OJK) grounded in the principles of the Electronic-Based Government System (SPBE). The proposed model establishes electronic system reliability as a normative supervisory standard for strengthening preventive legal protection and enhancing legal certainty for retail investors in Indonesia's digital investment ecosystem.

3. RESEARCH RESULT AND DISCUSSION

3.1. Legal Certainty in Protecting Retail Investors Against the Risk of Digital Investment System Failures

Indonesia has established a relatively comprehensive regulatory framework governing electronic systems and consumer protection in the financial services sector. Nevertheless, the existing regulatory regime remains fragmented and sector-specific, lacking an integrated framework capable of establishing operational standards for electronic system reliability as the legal basis for determining the liability of digital investment service providers. Consequently, investor protection continues to rely predominantly on ex post remedies after losses have occurred, whereas preventive regulatory mechanisms designed to mitigate such risks remain insufficiently developed.

Article 15(1) of the Electronic Information and Transactions (ITE) Law requires every Electronic System Operator (ESO) to operate electronic systems in a reliable, secure, and accountable manner. This obligation is reinforced by Government

Regulation No. 71 of 2019, which requires operators to implement business continuity plans (BCPs), disaster recovery plans (DRPs), information security management systems, and information technology risk management mechanisms. However, these regulations impose only general normative obligations and do not establish measurable operational standards for evaluating whether an electronic system satisfies legally acceptable reliability requirements. In particular, the regulatory framework does not specify minimum system availability, maximum permissible downtime, service interruption thresholds, or objective performance indicators that would enable regulators or courts to determine whether a system failure constitutes a breach of legal obligations. As a result, when failures occur on digital investment platforms, retail investors often encounter significant evidentiary challenges in proving provider negligence because no objective legal benchmarks exist against which system performance can be assessed.

This regulatory deficiency illustrates the absence of operational legal norms. According to Kelsen, legal obligations can generate effective accountability only when legal norms prescribe clear, measurable, and consistently enforceable legal consequences.⁹ Although Article 15 of the ITE Law establishes a general obligation to maintain reliable electronic systems, it does not provide normative criteria enabling supervisory authorities or courts to determine when system disruptions amount to violations of legal duties.

Accordingly, the provision functions primarily as a programmatic norm rather than an operational norm. As Radbruch argues, the existence of legal norms alone does not ensure legal certainty unless those norms clearly define rights, obligations, and their corresponding legal consequences.¹⁰ While investors understand that electronic system providers are legally required to maintain reliable systems, the law does not specify the minimum reliability standards to which investors are entitled. This regulatory ambiguity weakens legal certainty and complicates the enforcement of provider accountability.

Comparable deficiencies are evident within the financial services regulatory framework. This study finds that Financial Services Authority (OJK) Regulation No. 11/POJK.03/2022 concerning information technology implementation applies exclusively to commercial banks. However, most retail investors now conduct investment transactions through wealth technology (wealthtech) applications, online brokerage platforms, investment marketplaces, securities companies, Mutual Fund Selling Agents (APERDs), and financial technology service providers, all of which fall outside the scope of this regulation. Consequently, the relatively sophisticated information technology risk management standards applicable to the banking sector have not been uniformly extended to the broader digital investment ecosystem.

⁹ Hans Kelsen, *Pure Theory of Law* (University of California Press, 1967).

¹⁰ Gustav Radbruch, *Legal Philosophy* (Harvard University Press, 1950).

Furthermore, OJK Regulation No. 6/POJK.07/2022 requires Financial Services Business Actors to assume responsibility for the acts or omissions of third parties engaged in the provision of financial services. Nevertheless, the regulation does not establish evidentiary mechanisms for determining liability when service disruptions originate from cloud computing providers, data centers, communication networks, application programming interfaces (APIs), or other technology vendors. In practice, technical information regarding the root causes of system failures—including system logs, server records, cybersecurity reports, and information technology audit results—is controlled exclusively by service providers. Retail investors generally lack access to such technical evidence, thereby creating a significant imbalance in the allocation of evidentiary burdens and substantially limiting their ability to establish provider negligence in legal proceedings.

The findings of this study support those of Rahmat et al., which conclude that legal protection for retail investors in Indonesia's digital capital market remains heavily dependent on the good faith of service providers rather than on enforceable legal obligations supported by objective regulatory standards.¹¹ However, this study identifies a more fundamental regulatory deficiency. The principal weakness lies not merely in ineffective regulatory enforcement but in the absence of legally defined reliability standards that can serve as objective benchmarks for supervisory evaluation. Without measurable legal parameters governing electronic system reliability, the Financial Services Authority (OJK) lacks an adequate normative basis for conducting preventive supervision of the technological infrastructure operated by digital investment service providers. Consequently, the existing regulatory framework remains predominantly reactive, addressing investor losses only after system failures occur rather than preventing such losses through ex ante technology-based supervision.

The absence of clear operational standards has facilitated the widespread use of exoneration clauses in the terms and conditions of digital investment platforms. Most digital investment service providers include contractual provisions disclaiming liability for losses arising from system failures, scheduled server maintenance, internet connectivity disruptions, or events classified as technical force majeure. This practice is inconsistent with Article 18(1)(a) of Law No. 8 of 1999 on Consumer Protection, which expressly prohibits business actors from transferring their legal responsibilities to consumers through standard contractual clauses. From a normative perspective, such clauses are null and void. Nevertheless, their invalidity does not automatically provide effective legal protection for investors because the burden of proving provider negligence remains with the investor, who must pursue a civil action to obtain compensation.

¹¹ Rahmat et al., "Perlindungan Hukum Bagi Investor Ritel Dalam Transaksi Efek Di Pasar Modal Indonesia."

These findings are consistent with those of Setiadi and Utari, who concluded that exoneration clauses used by online Mutual Fund Selling Agent (APERD) platforms are legally unenforceable when they conflict with the Consumer Protection Law. However, the present study identifies a more fundamental issue.¹² The principal challenge is no longer the formal validity of exoneration clauses but the limited effectiveness of the existing investor protection framework, which remains predominantly litigation-oriented. Investors generally receive legal protection only after suffering financial losses and engaging in dispute resolution or civil litigation, both of which require considerable time, financial resources, and access to highly technical evidence. This situation demonstrates that Indonesia's regulatory framework continues to emphasize *ex post legal* remedies rather than *ex ante* preventive regulatory protection.

Philipus M. Hadjon distinguishes between preventive and repressive legal protection. The findings of this study indicate that Indonesia's regulatory framework for digital investment primarily emphasizes repressive mechanisms, including complaint procedures, dispute resolution, and civil litigation after investor losses have occurred.¹³ By contrast, preventive regulatory instruments—such as mandatory periodic information technology audits, legally defined electronic system reliability indicators, compulsory reporting of system availability, information security certification, and real-time supervisory monitoring—remain insufficiently regulated. Consequently, investors' statutory right to a reliable electronic system remains largely declaratory rather than operational because it is not supported by supervisory mechanisms capable of preventing system failures before they occur.

This study also extends the recommendations advanced by Lubis et al. (2026), who proposed mandatory information technology audits and certification for non-bank financial institutions based on internationally recognized standards such as ISO/IEC 27001. The present study argues that information technology audits alone are insufficient unless they are embedded within the Financial Services Authority's (OJK) regulatory framework through legally enforceable operational standards. Such standards should include measurable system availability requirements, Recovery Time Objectives (RTOs), continuous real-time monitoring of system resilience, mandatory incident reporting to regulators, and transparent disclosure of significant information technology failures. Within this framework, information technology audits should no longer be regarded merely as instruments of administrative compliance but rather as integral components of a preventive, technology risk-based supervisory system.

Accordingly, legal certainty for retail investors with respect to losses arising from failures of digital investment service systems has not yet been fully achieved. The

¹² Muhammad Rizky Setiadi and Indah Sri Utari, "Penerapan Klausula Eksonerasi Pada Syarat Dan Ketentuan Pengguna M-Banking," in *Bookchapter Hukum Dan Lingkungan*, vol. 1 (Universitas Negeri Semarang, 2025).

¹³ Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya* (Bina Ilmu, 1987).

existing regulatory framework continues to exhibit a significant normative gap between broadly stated legal obligations and the operational standards necessary to implement and enforce those obligations effectively. Investor protection cannot be adequately secured solely through the prohibition of exoneration clauses or reliance on post-loss litigation mechanisms. Instead, it requires a comprehensive reconstruction of the supervisory framework capable of integrating cybersecurity regulation with financial services regulation.

Therefore, the legal framework established under the Electronic Information and Transactions (ITE) Law, the Consumer Protection Law, the Law on the Development and Strengthening of the Financial Sector (P2SK Law), and the relevant Financial Services Authority (OJK) regulations on information technology governance should be reoriented toward establishing measurable, auditable, and continuously monitored standards for electronic system reliability. Such standards should form the normative foundation for technology-based supervision by the OJK. Under this approach, legal certainty would no longer function merely as a reactive mechanism for resolving disputes after investor losses occur but would instead evolve into a preventive regulatory instrument designed to ensure the reliability and resilience of digital investment systems while strengthening investor confidence in Indonesia's rapidly expanding digital capital market ecosystem.

3.2. Reconstructing the Financial Services Authority's Supervisory Architecture Through the Integration of Electronic-Based Government System (SPBE) Principles

Indonesia already possesses a sufficiently robust normative foundation to develop such a supervisory model without requiring the enactment of new legislation. The principal challenge lies not in the absence of a legal basis but in the lack of integration among the cybersecurity regulatory framework, digital governance principles, and financial services regulations into a coherent and unified digital supervisory architecture.

Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE) establishes the fundamental principles governing electronic government systems, including effectiveness, integration, security, reliability, interoperability, efficiency, and accountability. These seven principles extend beyond administrative standards for public institutions and embody universally recognized principles of modern electronic system governance.

Among these principles, reliability, security, and interoperability are particularly relevant to the operation of digital investment platforms, which depend heavily on uninterrupted service delivery and the seamless integration of multiple information technology infrastructures. More importantly, Presidential Regulation No. 132 of 2022 concerning the National SPBE Architecture designates the Financial Services Authority

(OJK) as one of the public institutions required to implement supervisory systems consistent with the national SPBE architecture. Consequently, the OJK is itself legally obligated to comply with SPBE principles, including electronic system reliability, in the design and implementation of its supervisory functions.

Accordingly, the legal issue is no longer whether the OJK may rely on SPBE principles as the normative basis for supervising the financial services sector, but rather how those principles can be translated into enforceable administrative standards applicable to digital financial service providers. The legal authority for such a transformation is provided by Articles 213 and 245 of Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector (P2SK Law), which authorize the OJK to regulate Financial Sector Technology Innovation (ITSK), establish technological standards, and develop risk-based supervisory mechanisms. Because the SPBE framework is formally intended to govern public institutions, its principles need not be imposed directly as statutory obligations on private-sector entities. Instead, the substantive values embodied in the SPBE framework can be incorporated through the OJK's regulatory authority by establishing administrative requirements for the licensing, supervision, and continued operation of digital investment platform providers.

This approach represents a fundamental shift in the regulatory paradigm—from compliance-based supervision to technology-driven preventive supervision. Traditionally, OJK supervision has relied primarily on administrative compliance, periodic inspections, and routine reports submitted by financial service providers. Although this supervisory model has proven relatively effective within conventional financial systems, it is increasingly inadequate for regulating digital investment platforms, where operational conditions may change within seconds and technology-related risks emerge in real time.

Accordingly, digital supervision should be reconstructed through the adoption of Supervisory Technology (SupTech), which integrates advanced data analytics, continuous real-time monitoring, automated regulatory reporting, and data interoperability across regulated entities. Such a framework would enable regulators to maintain a continuous and comprehensive understanding of the operational condition and resilience of electronic systems supporting digital investment services. This finding is consistent with the observations of Setiawan and Nugroho, who argue that contemporary financial regulators can no longer rely exclusively on formal administrative compliance but must adopt data-driven supervisory approaches capable of dynamically identifying and mitigating emerging technological risks.¹⁴ Under this model, regulatory oversight becomes preventive rather than reactive, allowing supervisory authorities to detect potential system vulnerabilities before they result in

¹⁴ Muhammad Thoriq Setiawan and Rino Ardhian Nugroho, "Analisis E-Government Dalam Penerapan Aplikasi Solodata Di Dinas Komunikasi, Informatika, Statistik, Dan Persandian (DISKOMINFO SP) Kota Surakarta," *Wacana Publik* 5, no. 1 (2025): 161–73, <https://doi.org/10.20961/wp.v5i1.104044>.

investor losses and thereby strengthening legal certainty within Indonesia's digital investment ecosystem.

This study proposes an operational model for integrating the principles of the Electronic-Based Government System (SPBE) into the Financial Services Authority's (OJK) Supervisory Technology (SupTech) framework through three sequential stages.

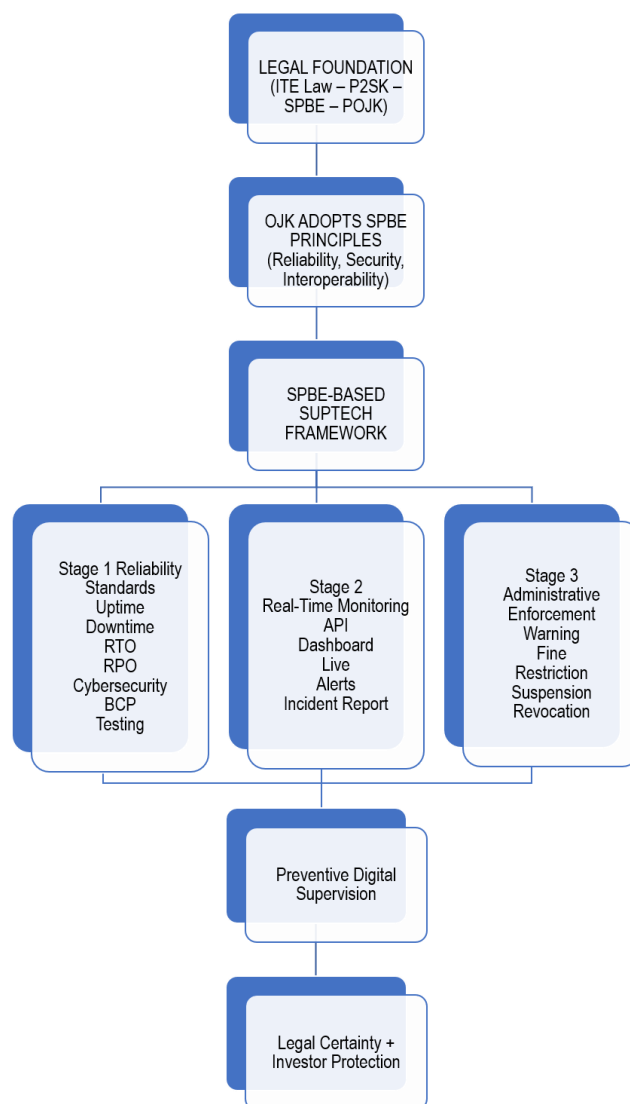


Figure 1. Proposed SPBE-Based SupTech Supervisory Model for Strengthening Legal Protection of Retail Investors

The first stage involves establishing electronic system reliability standards as concrete operational manifestations of the SPBE principle of reliability. These standards should include measurable performance indicators, such as minimum system availability (uptime), maximum allowable downtime, Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), mandatory reporting of information technology incidents within prescribed timeframes, cybersecurity requirements, and compulsory business continuity testing. The findings indicate that these operational indicators are not explicitly regulated under the existing Financial Services Authority regulations (POJK).

Accordingly, this study recommends either the enactment of a new POJK or the revision of POJK No. 11/POJK.03/2022 to extend its scope beyond the banking sector to encompass all digital investment service providers, including securities companies, Mutual Fund Selling Agents (APERDs), wealth technology (wealthtech) platforms, and Financial Sector Technology Innovation (ITSK) providers.

The second stage focuses on developing a real-time electronic system reliability reporting mechanism through the OJK's SupTech infrastructure. Drawing upon the SPBE principle of interoperability, this study proposes that every digital investment platform be required to integrate its operational monitoring system with the OJK's supervisory platform through a secure and encrypted Application Programming Interface (API). Such integration would enable regulators to monitor critical operational indicators—including system availability, service disruptions, cybersecurity incidents, and transaction failures—in real time, eliminating reliance on periodic reporting. Continuous digital supervision would allow the OJK to identify operational anomalies promptly, implement timely supervisory interventions, and prevent localized system failures from escalating into widespread investor losses.

The third stage emphasizes strengthening administrative enforcement mechanisms. This study finds that the effectiveness of preventive legal protection depends largely on the existence of clear legal consequences for non-compliance with established technological standards. Accordingly, failure to satisfy prescribed electronic system reliability indicators should constitute an administrative violation subject to graduated sanctions, including written warnings, mandatory corrective measures, administrative fines, restrictions on business activities, and, in cases of repeated or serious non-compliance, the suspension or revocation of business licenses. Under this regulatory framework, investors would no longer bear the primary burden of initiating civil litigation to compel providers to fulfill their legal obligations. Instead, compliance with technological reliability standards would become an integral component of the OJK's administrative supervisory function.

The proposed model extends the recommendations advanced by Lubis et al., who advocated mandatory information technology audits and ISO/IEC 27001 certification for non-bank financial institutions.¹⁵ While audits and certification remain important regulatory instruments, this study argues that they are insufficient unless incorporated into a framework of continuous technology-based supervision through SupTech. Conventional audits are inherently periodic, whereas failures of electronic systems may occur at any time. Consequently, an effective supervisory framework should combine periodic compliance audits with continuous real-time digital monitoring, thereby

¹⁵ Muharman Lubis et al., "The Integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) Framework Effectiveness in the Non-Bank Financial Industry," *Computers* 15, no. 1 (2026): 60, <https://doi.org/10.3390/computers15010060>.

enabling regulators to detect operational irregularities at an early stage and implement preventive interventions before system failures adversely affect investors.

The proposed supervisory model is supported by strong theoretical foundations. From the perspective of utilitarian theory, as articulated by Bentham, imposing additional obligations relating to electronic system reliability standards and real-time digital reporting inevitably increases compliance costs for digital investment platform operators.¹⁶ Nevertheless, these additional regulatory burdens are substantially outweighed by the broader social benefits derived from protecting millions of retail investors, enhancing market stability, and strengthening public confidence in Indonesia's digital capital market. Accordingly, the proposed framework is consistent with Bentham's principle of achieving "the greatest happiness of the greatest number," as the collective benefits generated by preventive supervision exceed the incremental compliance costs imposed on regulated entities.

Furthermore, viewed through the lens of law as a tool of social engineering, as proposed by Kusumaatmadja, law should function not merely as a mechanism for resolving disputes after losses have occurred but also as an instrument for directing institutional and technological transformation within society.¹⁷ The integration of SPBE principles into the OJK's SupTech framework exemplifies this regulatory function by encouraging digital investment service providers to develop a culture of compliance grounded in operational resilience, technological reliability, and continuous risk management rather than mere formal adherence to administrative requirements. In this way, legal regulation becomes a proactive governance mechanism capable of shaping institutional behavior, strengthening preventive investor protection, and enhancing legal certainty within Indonesia's rapidly evolving digital financial ecosystem.

The European Union's Digital Operational Resilience Act (DORA) establishes digital operational resilience as a mandatory requirement for the licensing, governance, and ongoing supervision of financial institutions.¹⁸ Similarly, the Monetary Authority of Singapore (MAS), through its Technology Risk Management Guidelines, requires financial institutions to comply with comprehensive standards for system reliability, cyber resilience, and the continuous reporting of information technology incidents.¹⁹ These international regulatory developments are broadly consistent with Indonesia's evolving legal framework. The Electronic Information and Transactions (ITE) Law, the Law on the Development and Strengthening of the Financial Sector (P2SK Law), and the Electronic-Based Government System (SPBE) framework collectively provide an

¹⁶ Jeremy Bentham, *Utilitarianism* (Progressive Publishing Company, 1890).

¹⁷ Mochtar Kusumaatmadja, *Fungsi Dan Perkembangan Hukum Dalam Pembangunan Nasional* (Universitas Padjadjaran, 1970).

¹⁸ European Insurance and Occupational Pensions Authority, *Digital Operational Resilience Act (DORA)*, 2025, https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

¹⁹ Monetary Authority of Singapore, *Achieving Operational Resilience for Financial Institutions in Singapore*, 2020, <https://www.mas.gov.sg/regulation/operational-resilience>.

adequate normative foundation for strengthening digital financial supervision. Consequently, the implementation of a SupTech-based supervisory model does not require the enactment of new legislation. Rather, it requires technical and institutional harmonization between the Ministry of Communication and Digital, as the authority responsible for the national SPBE architecture, and the Financial Services Authority (OJK), as the regulator of Indonesia's financial services sector.

Accordingly, the reconstruction of the OJK's supervisory architecture through the integration of SPBE principles represents a model that is legally viable, administratively operational, and theoretically robust in addressing the deficiencies of Indonesia's existing digital investor protection framework, which remains predominantly reactive. The principal novelty of this study lies in its conceptualization of the SPBE framework not as a set of legal obligations imposed directly upon private-sector entities, but as a source of normative principles to be adopted by the Financial Services Authority (OJK) through its regulatory authority under the P2SK Law. These principles serve as the foundation for establishing electronic system reliability standards within a SupTech-based supervisory framework. The proposed model not only enhances legal certainty and clarifies the allocation of responsibilities among digital investment service providers but also fundamentally transforms the paradigm of investor protection by shifting the regulatory focus from *ex post* dispute resolution toward *ex ante*, technology-driven preventive supervision capable of adapting to the continuing digital transformation of Indonesia's financial services sector.

4. CONCLUSION

Although the Electronic Information and Transactions (ITE) Law, the Consumer Protection Law, the Law on the Development and Strengthening of the Financial Sector (P2SK Law), and various Financial Services Authority (OJK) regulations (POJK) provide a normative framework for investor protection, they continue to exhibit significant regulatory gaps regarding operational standards for electronic system reliability, objective criteria for determining system failures, and the allocation of liability among participants within the digital investment ecosystem. This study argues that the SPBE principle of reliability can be reconstructed as an administrative regulatory standard through the OJK's authority under the P2SK Law to develop a Supervisory Technology (SupTech) framework that supports real-time supervision, measurable service-level standards, and risk-based regulatory enforcement. In doing so, the study contributes to the advancement of a more preventive approach to both cybersecurity law and financial services regulation.

This study is subject to certain limitations. Specifically, it adopts a normative legal research approach and does not empirically examine the implementation of SupTech within the OJK's supervisory framework. Accordingly, it is recommended that the Government of Indonesia and the OJK develop or revise relevant POJK regulations to

establish measurable standards for electronic system reliability and strengthen institutional coordination with the Ministry of Communication and Digital. Future research should employ empirical and comparative methodologies to evaluate the effectiveness of the proposed SupTech-based supervisory model and to assess its consistency with internationally recognized regulatory best practices.

REFERENCES

Journals

- Bari, Abdulbari, and Putri Raodah. "Perlindungan Hukum Terhadap Investor Dalam Kegiatan Investasi Digital Di Indonesia." *Commerce Law* 4, no. 1 (2024): 61–69. <https://doi.org/10.29303/commercelaw.v4i1.4693>.
- Jiang, Hui. "How Does Computing Infrastructure Deployment Drive Corporate Digital Technology Innovation?" *Finance Research Letters* 86 (2025): 108659. <https://doi.org/10.1016/j.frl.2025.108659>.
- Lim, Feili. "Perlindungan Hukum Bagi Investor Dalam Era Transformasi Digital: Kajian Hukum Bisnis Di Indonesia." *Media Hukum Indonesia* 3, no. 4 (2025): 93–97. <https://doi.org/10.5281/ZENODO.17263115>.
- Lubis, Muharman, Muhammad Irfan Luthfi, Rd. Rohmat Saedudin, Alif Noorachmad Muttaqin, and Arif Ridho Lubis. "The Integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) Framework Effectiveness in the Non-Bank Financial Industry." *Computers* 15, no. 1 (2026): 60. <https://doi.org/10.3390/computers15010060>.
- Maulana, Mohamad Rafi, and Achmad Hariri. "Perlindungan Hukum Bagi Investor Ritel Terhadap Praktik Insider Trading Di Pasar Modal." *Jurnal Ilmiah Advokasi* 14, no. 1 (2026): 90–107. <https://doi.org/10.36987/jiad.v14i1.6995>.
- Mukhlisin, Raden Muhammad. "Transformasi Hukum Pasar Modal Di Era Digital: Pilar Investasi Dan Pembangunan Ekonomi." *Yustisi* 12, no. 3 (2025): 175–89. <https://doi.org/10.32832/yustisi.v12i3.19858>.
- Mustovich, Munna Hidayatul, Nabela Uqbal Kuroma, and Afiana Mu'arifah. "Perlindungan Hukum Bagi Investor Ritel Dalam Perubahan Efek Syariah Pasca Pojk Nomor 8 Tahun 2025 Di Pasar Modal Syariah Indonesia." *Syariah: Jurnal Ilmu Hukum* 3, no. 4 (2026): 310–18. <https://doi.org/10.62017/syariah.v3i4.8560>.
- Rahmat, Rahmat, Dinda Aditya Winanda, Nazwa Naila Pasaribu, Dita Amanda Hafizah, and Fadya Rahazri Meyfiza. "Perlindungan Hukum Bagi Investor Ritel Dalam Transaksi Efek Di Pasar Modal Indonesia." *Jurnal Analisis Hukum Dan Kebijakan* 6, no. 2 (2025): 162–70.
- Ridwan, Mochammad Samsi. "Perlindungan Hukum Investor Ritel Dalam Perdagangan Aset Keuangan Digital Pasca POJK Nomor 23 Tahun 2025."

Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory 4, no. 2 (2026): 1514–46. <https://doi.org/10.62976/ijijel.v4i2.1829>.

Setiawan, Muhammad Thoriq, and Rino Ardhian Nugroho. “Analisis E-Government Dalam Penerapan Aplikasi Solodata Di Dinas Komunikasi, Informatika, Statistik, Dan Persandian (DISKOMINFO SP) Kota Surakarta.” *Wacana Publik* 5, no. 1 (2025): 161–73. <https://doi.org/10.20961/wp.v5i1.104044>.

Vijayaputro, Muhammad Raditya. “Perlindungan Hukum Mengenai Investasi Digital Dalam Bentuk Non-Fungible Token Berdasarkan Undang-Undang Nomor 25 Tahun 2007.” *Unes Law Review* 6, no. 2 (2023): 4397–402. <https://doi.org/10.31933/unesrev.v6i2.1276>.

Yuniarti, Erika, and Bayu Mahatma. “Perlindungan Hukum Terhadap Investor Dalam Investasi Digital Di Indonesia: Analisis Kebijakan Dan Tantangan Regulasi Di Era Digital.” *Simpul: Jurnal Ilmu Politik Dan Hukum* 1, no. 2 (2025): 30–36. <https://doi.org/10.71094/simpul.v1i2.128>.

Books

Bentham, Jeremy. *Utilitarianism*. Progressive Publishing Company, 1890.

Kelsen, Hans. *Pure Theory of Law*. University of California Press, 1967.

Kusumaatmadja, Mochtar. *Fungsi Dan Perkembangan Hukum Dalam Pembangunan Nasional*. Universitas Pedjajaran, 1970.

Philipus M. Hadjon. *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya*. Bina Ilmu, 1987.

Radbruch, Gustav. *Legal Philosophy*. Harvard University Press, 1950.

Setiadi, Muhammad Rizky, and Indah Sri Utari. “Penerapan Klausula Eksonerasi Pada Syarat Dan Ketentuan Pengguna M-Banking.” In *Bookchapter Hukum Dan Lingkungan*, vol. 1. Universitas Negeri Semarang, 2025.

Web Pages

European Insurance and Occupational Pensions Authority. *Digital Operational Resilience Act (DORA)*. 2025. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

Monetary Authority of Singapore. *Achieving Operational Resilience for Financial Institutions in Singapore*. 2020. <https://www.mas.gov.sg/regulation/operational-resilience>.