

Reformulation of the Law on Financial System Stability Supervision Against the Risk of Digital Crisis and Economic Disruption as an Effort to Strengthen State Capacity Towards Golden Indonesia 2045

Ridwan Mohamad Faisal *, Yopik Gani, Kif Aminanto

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; ridwanmohamadfaisal@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; yopikgadi@gmail.com

Sekolah Tinggi Ilmu Kepolisian, South Jakarta, Indonesia ; kif.92pw@gmail.com

DOI:

<https://doi.org/10.47134/jcl.v3i3.2.6325>

*Correspondence: Ridwan Mohamad Faisal

Email:

ridwanmohamadfaisal@gmail.com

Received: 08/08/2026

Accepted: 27/08/2026

Published: 31/08/2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY-SA) license (<http://creativecommons.org/licenses/by-sa/4.0/>).

Abstract: *The digital economic transformation has changed the structure of the national financial system and given rise to various new forms of risks that have the potential to disrupt national macroeconomic stability, such as cyber attacks on the financial sector, digital bank runs, financial data leaks, digital asset volatility, and the dominance of global technology platforms in payment systems and economic transactions. This study aims to analyze the weaknesses of the legal framework for financial system stability supervision in Indonesia in the face of the risk of a digital crisis, examine the relationship between institutional resilience and state capacity on macroeconomic stability, and formulate a legal reformulation of financial system stability supervision based on digital risks towards Indonesia Emas 2045. This study employs a normative juridical method with legislative and conceptual approaches through an analysis of the Bank Indonesia Law, the Financial Services Authority Law, the Financial System Crisis Prevention and Management Law, the Electronic Information and Transactions Law, and the Personal Data Protection Law. The results of the study indicate that the legal system for financial supervision in Indonesia still faces fragmentation of authority, weak institutional coordination, limited cyber resilience regulations, and the absence of integrated digital financial supervision capable of comprehensively anticipating digital threats. Therefore, legal reform is needed through strengthening cyber financial governance, establishing a digital crisis management framework, integrating a national early warning system, strengthening financial data protection, and developing an adaptive, responsive, and resilient digital financial oversight system to strengthen the state's capacity to maintain macroeconomic stability towards Indonesia Emas 2045.*

Keywords: *financial system stability, digital risk, institutional resilience, state capacity, Indonesia Emas 2045.*

Introduction

The digital economic transformation has fundamentally changed the structure of Indonesia's national financial system. The development of financial technology (fintech), digital banking, cryptocurrency, artificial intelligence in financial services, open banking, and embedded finance has rapidly and massively expanded public access to financial services (Sinaga, 2025). This phenomenon is reinforced by the acceleration of digitalization after the COVID-19 pandemic, which has driven changes in people's transaction behavior from conventional systems to electronic transactions based on digital platforms. Bank

Indonesia recorded a significant increase in electronic money, digital banking, and QRIS transactions as an indicator of the public's increasing dependence on digital financial infrastructure (Widyasari, R., & Hermawan, 2024). Normatively, this development is legally legitimized through Law Number 23 of 1999 concerning Bank Indonesia, as most recently amended by Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, specifically Article 8, which authorizes Bank Indonesia to maintain the stability of the rupiah and the national payment system. Furthermore, Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector also expands the regulatory space for technological innovation in the financial sector and oversight of the digitalization of the national financial system (Rahayu, N., Supriyono, I. A., Mulyawan, E., Nurfadhillah, F., Yulianto, D. R., Ramadhan, 2023). However, the digitalization of the financial system not only brings economic efficiency but also creates new forms of vulnerability distinct from those characteristic of conventional financial crises. The country's dependence on digital systems means that national economic stability is no longer solely determined by macroeconomic fundamentals but is also heavily influenced by cybersecurity, data integrity, and the resilience of financial technology. This situation demonstrates that digital transformation has expanded the dimensions of financial system stability from merely monetary and banking issues to the resilience of the country's digital infrastructure.

The development of the digital economy has subsequently given rise to various forms of digital crisis risks that may potentially disrupt the stability of the national financial system. These risks include cyberattacks on banking and national payment systems, leaks of financial data, failures of electronic payment systems, artificial intelligence manipulation in financial transactions, digital shadow banking, crypto-asset volatility, illegal online lending, and the possibility of digital bank runs resulting from the rapid dissemination of information through social media (Rahakbauw, 2024). Because this study employs a normative juridical method, these phenomena are not presented as independent quantitative findings of the research, but as contextual developments discussed in relevant academic literature and used to examine the adequacy of the existing legal framework.

The normative problem examined in this study concerns whether Indonesian law has developed an integrated legal mechanism capable of addressing risks that originate from or are amplified through digital infrastructure. Regulations regarding data protection and electronic systems are regulated through Law Number 27 of 2022 concerning Personal Data Protection and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, specifically Articles 30, 32, and 46 concerning illegal access and manipulation of electronic systems (Syah, E., Weharima, H., Susilo, T., Basuki, T., & Akad, 2025). However, these regulations primarily regulate electronic systems, personal data, and cyber-related violations and do not yet establish an integrated legal framework for identifying, classifying, and managing systemic digital financial risks.

Therefore, the issue addressed by this study is not the statistical frequency of every digital incident, but the normative gap between the technological characteristics of emerging financial risks and the legal architecture governing financial system stability, institutional coordination, cyber resilience, and crisis intervention.

On the other hand, the legal framework for financial system stability oversight in Indonesia still exhibits various structural weaknesses that prevent the country from having adequate legal capacity to address the risks of digital crises. Current financial sector oversight regulations are still scattered across various institutional regimes, including Bank Indonesia under the Bank Indonesia Law, the Financial Services Authority under Law Number 21 of 2011 concerning the Financial Services Authority, the Ministry of Finance, the Ministry of Communication and Digital, and the National Cyber and Crypto Agency under Presidential Regulation Number 53 of 2017 (Abrini, R. P., & Paraya, 2020).

This fragmentation of authority results in digital risk oversight that remains institutionally segmented and lacks a legally structured mechanism for systemic digital integration. Article 39 of Law Number 9 of 2016 concerning the Prevention and Management of Financial System Crises establishes the Financial System Stability Committee (KSSK); however, the existing formulation does not expressly include systemic digital financial risk, cybersecurity incidents affecting financial infrastructure, large-scale payment-system disruption, algorithmic financial instability, or digital contagion as categories requiring coordinated crisis assessment (Parulian, 2021).

Article 44 of Law Number 9 of 2016 provides a basis for coordination among relevant financial authorities, but the existing coordination framework does not establish a specific obligation for real-time digital-risk information sharing, standardized interoperability, joint validation of systemic digital threats, or a legally defined escalation mechanism when a digital incident crosses institutional jurisdictions. Consequently, the legal issue is not merely the existence of KSSK, but the absence of an explicit digital-risk architecture within its statutory mandate (Asiyanti, A. P., & Agussalim, 2024).

Legal reform should therefore amend Article 39 by expressly expanding the scope of KSSK coordination to include the assessment and management of systemic digital financial risks and digital financial crises. Article 44 should be reformulated to establish a structured coordination mechanism consisting of mandatory incident notification, legally defined categories of shareable data, interoperable information exchange, joint risk assessment, escalation procedures, and documented institutional responsibilities. Such reform would strengthen KSSK as a coordinating mechanism without transferring the original regulatory and supervisory powers of Bank Indonesia, OJK, or other competent institutions.

Another crucial problem is the weak coordination between state institutions in addressing digital systemic risk. In practice, digital financial supervision often faces overlapping authority between institutions, bureaucratic sectoral egos, slow data exchange, and suboptimal integration of the national early warning system. Despite the fact that digital threats differ significantly from conventional threats because they move quickly, simultaneously, and can cross jurisdictional boundaries in a matter of seconds (Gunibala, 2025). Provisions regarding institutional coordination are actually regulated through Article 44 of Law Number 9 of 2016 concerning the Prevention and Management of Financial System Crises, which assigns a coordinating function to the Financial System Stability Committee (KSSK). However, empirically, this coordination mechanism still faces limitations in digital oversight interoperability and is not supported by an adequate national data integration system (Asiyanti, A. P., & Agussalim, 2024). In cyber financial governance,

conventional coordination based on administrative bureaucracy is no longer sufficient to address highly dynamic digital threats. The country requires a technology-based coordination model, real-time data integration, and a rapid response system capable of simultaneously connecting monetary authorities, financial services authorities, digital regulators, and cybersecurity agencies. Without institutional coordination reform, the potential for digital crises will become increasingly difficult to control and could disrupt national economic stability broadly.

In addition to domestic factors, Indonesia's financial system stability also faces global pressures due to increasingly complex international economic disruptions. Geopolitical conflicts, trade wars, global recessions, economic deglobalization, economic cyberwarfare, and changes in the international financial architecture resulting from the development of central bank digital currencies (CBDCs) and digital currencies have created new uncertainties in the global economic system. As a developing country, Indonesia is highly vulnerable to external shocks, particularly as the integration of the national economy with the international financial system is increasingly digital (Aji, 2023). The dominance of transnational technology platforms also increases the risk of national economic dependence on foreign infrastructure, which is difficult for the state to effectively monitor. From the perspective of constitutional economic law, this situation indicates that macroeconomic stability can no longer be understood solely within the framework of conventional fiscal and monetary policies, but must instead be viewed as part of the state's institutional resilience (Simbolon, M. M., Kesuma, I. G., & Wibowo, 2021). State capacity theory places regulatory, administrative, technological, supervisory, and crisis response capabilities as key elements of a modern state's success in maintaining national stability (Dzikri, 2016). Therefore, the state must possess institutional resilience that is not only normatively strong but also adaptive to technological change and global digital threats.

Based on these conditions, legal reformulation of digital risk-based financial system stability supervision is an urgent need to strengthen the state's capacity towards the Vision of a Golden Indonesia 2045. Legal reform is needed to establish integrated digital financial supervision that can integrate monetary supervision, financial services sector supervision, cybersecurity, data protection, and digital systemic risk control in an integrated manner. These reforms must be directed at establishing cyber financial governance based on adaptive regulation, strengthening the national regulatory sandbox, establishing a digital crisis management framework, and strengthening the legal basis for coordination between state institutions. From the perspective of progressive and responsive law, regulations should not merely function as an instrument of administrative control, but must also be able to anticipate technological developments and global risk dynamics. Therefore, the reformulation of the law on financial system stability supervision aims not only to maintain national economic resilience but also to serve as a strategic instrument in building the capacity of a modern state that is adaptive, resilient, and capable of supporting sustainable development towards Indonesia Emas 2045.

Methodology

This research employs a normative juridical research method that focuses on the study of legal norms, legal principles, the synchronization of laws and regulations, and legal

concepts related to the supervision of financial system stability in the face of the risks of digital crises and economic disruption. The approaches employed include a statutory approach and a conceptual approach. The legislative approach examines various regulations related to financial system stability, supervision of the financial services sector, cybersecurity, personal data protection, and digital transformation of the economic sector, including Law Number 23 of 1999 concerning Bank Indonesia as last amended by Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector, Law Number 21 of 2011 concerning the Financial Services Authority, Law Number 9 of 2016 concerning Prevention and Handling of Financial System Crises, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 1 of 2024. Meanwhile, a conceptual approach is used to analyze the theory of state capacity, institutional resilience, cyber financial governance, adaptive regulation, and the concept of macroeconomic stability in a modern rule of law to build legal arguments regarding the urgency of reformulating the law on supervision of the stability of the financial system based on digital risk. The legal materials used consist of primary legal materials, secondary legal materials, and tertiary legal materials, which are analyzed prescriptively using legal interpretation and legal construction techniques to produce a legal reform formulation that is responsive, adaptive, and oriented towards strengthening state capacity towards Golden Indonesia 2045.

Result and Discussion

Analysis of Weaknesses in the Legal Framework for Financial System Stability Supervision in Facing the Risk of Digital Crisis and Economic Disruption in Indonesia

The digital economic transformation has fundamentally changed the structure of Indonesia's national financial system, but this development has not been fully matched by an adequate legal framework for financial system stability oversight. The Indonesian financial sector legal system is still fundamentally built on a conventional supervisory paradigm oriented toward monetary stability, banking, and traditional financial services institutions. However, the digitalization of the financial sector through fintech, digital banks, crypto assets, artificial intelligence, and electronic payment platforms has transformed the nature of systemic risk, making it more complex, rapid, interconnected, and cross-jurisdictional (Sudiantini, D., Ayu, M. P., Aswan, M. C., Prastuti, M. A., & Apriliya, 2023).

For the purpose of legal reformulation, systemic digital financial risk should be understood as a risk arising from, transmitted through, or substantially amplified by digital infrastructure, electronic financial systems, algorithmic processes, interconnected digital platforms, or large-scale digital data disruptions, where the risk has the potential to impair the stability, continuity, integrity, or public confidence of a significant part of the national financial system. A digital financial crisis, in turn, should be defined as a condition in which one or more systemic digital financial risks have materialized or are reasonably expected to materialize and require coordinated extraordinary measures to prevent serious disruption to financial system stability.

These concepts must be distinguished from an ordinary cybersecurity incident, which may affect a particular institution without producing systemic consequences; an operational failure, which concerns the malfunction of a specific service or infrastructure; conventional banking crises, which primarily arise from liquidity, solvency, or institutional financial distress; and ordinary financial-market volatility, which remains within normal market fluctuation. The defining element of systemic digital financial risk is therefore not merely the existence of technology or a cyber incident, but the combination of digital disruption, interconnection, propagation potential, and the capacity to create significant consequences for financial system stability. Although the existing legal framework includes Law Number 23 of 1999 concerning Bank Indonesia as amended by Law Number 4 of 2023, Law Number 21 of 2011 concerning the Financial Services Authority, and Law Number 9 of 2016 concerning the Prevention and Management of Financial System Crises (Purba, 2024), these regulations do not yet provide an explicit legal formulation addressing this category of systemic digital risk.

One of the main weaknesses of the legal framework for overseeing financial system stability in Indonesia lies in the fragmentation of authority among state institutions, resulting in partial and unintegrated digital supervision. Bank Indonesia holds authority over monetary and payment systems under Article 8 of the Bank Indonesia Law, while the Financial Services Authority, under Article 6 of Law Number 21 of 2011, has regulatory and supervisory authority over the financial services sector. On the other hand, data protection and electronic systems fall under the authority of the Ministry of Communication and Digital under Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024. National cybersecurity falls under the purview of the National Cyber and Crypto Agency under Presidential Regulation Number 53 of 2017 concerning the National Cyber and Crypto Agency. This fragmentation of authority has led to overlapping authority and supervisory disharmony in addressing multidimensional digital threats. In practice, there is no mechanism for integrating real-time supervision between institutions to detect systemic digital financial risk quickly and comprehensively (Sjofjan, L., Al-Fikri, M. F., Farisqi, M. R., Atha, M., & Saputra, 2025). This situation demonstrates that Indonesia's financial oversight institutional design is still based on separate administrative sectors, even though digital risks require an integrated financial supervision model that is cross-sectoral and cross-technological.

Another weakness lies in the suboptimal regulation of cyber resilience within the national financial system. To date, Indonesia lacks specific regulations that comprehensively address the cyber resilience of the financial sector as an integral part of the stability of the national financial system. Indeed, there are some partial regulations, such as Articles 30 and 32 of the Electronic Information and Transactions Law concerning illegal access and manipulation of electronic systems, and Law Number 27 of 2022 concerning Personal Data Protection, which regulates the protection of personal data in electronic systems. However, these regulations do not yet establish a legal framework for cyber financial governance integrated with financial system stability policies. Cyber-attacks on banks, customer data leaks, ransomware on digital payment infrastructure, and financial

cloud system failures can trigger a crisis of public confidence in the national financial system (Fitrianto, 2025). In this case, cyber threats are no longer merely information technology crimes but have evolved into systemic threats to national economic stability. The absence of regulations specifically addressing cyber resilience obligations for financial institutions demonstrates the weak preventive orientation of Indonesian law in addressing systemic digital risks.

Furthermore, oversight of fintech, digital assets, and digital shadow banking still faces significant legal gaps. Fintech regulation in Indonesia largely takes the form of sectoral administrative regulations through Financial Services Authority Regulations and Bank Indonesia Regulations, while financial technology developments are proceeding far faster than the country's legislative capabilities. Crypto assets, for example, were once in a regulatory gray area because they were not recognized as a means of payment under Article 1, number 2 of Law Number 7 of 2011 concerning Currency, yet they were traded as digital commodities under the policies of the Commodity Futures Trading Regulatory Agency. This regulatory disharmony demonstrates the absence of a comprehensive legal grand design for overseeing the integration of digital technology with the stability of the national financial system. A similar problem also occurs with the phenomenon of illegal online lending, which continues to grow due to weak oversight across digital platforms and limited legal jurisdiction over foreign-based applications. Under certain conditions, digital shadow banking even has the potential to create a parallel financial intermediation system outside the supervision of official state authorities, thereby increasing the risk of systemic financial instability (Azizah, 2025). Therefore, the weak regulation of fintech and digital assets demonstrates that Indonesia's financial sector law is still lagging behind the global digital economic transformation.

Another crucial issue is the inadequate legal protection of public financial data, which is essential for the stability of the national financial system. In the digital economy era, financial data holds a strategic position as it serves as the basis for economic decision-making, credit activities, risk analysis, and even control of the national payment system. Leaks of public financial data not only harm individuals but can also create a crisis of public trust in financial institutions and the country's economic system. Law Number 27 of 2022 concerning Personal Data Protection regulates the rights of data subjects and the obligations of data controllers, specifically Article 35 concerning the obligation to protect personal data and Article 46 concerning administrative sanctions. However, these regulations do not specifically address financial data as strategic national financial data with a macroeconomic stability dimension (Satria, M., & Handoyo, 2022). Furthermore, the dominance of global technology companies in controlling Indonesians' digital transaction data also raises issues of data sovereignty and limited state oversight jurisdiction. The situation demonstrates that national law is unable to establish a financial data protection system integrated with the resilience of the national financial system and the country's economic security.

The weakness of the legal framework for financial system stability oversight in Indonesia ultimately demonstrates the unpreparedness of the national legal system to address the fast-moving, complex, and transnational nature of digital threats. Law Number

9 of 2016 concerning the Prevention and Management of Financial System Crises does establish the Financial System Stability Committee (KSSK) through Article 39 as a coordination forum among state financial authorities. However, this mechanism remains oriented toward conventional economic crises and has not integrated a technology-based digital oversight system. Yet, threats such as digital bank runs resulting from the massive dissemination of information on social media, artificial intelligence manipulation in financial markets, and attacks on national payment infrastructure can develop far faster than conventional state bureaucratic responses. Thus, there is a pressing urgency to reformulate the law on financial system stability oversight through the establishment of integrated digital financial supervision, strengthening cyber financial governance, harmonizing cross-sectoral regulations, and developing a responsive legal framework based on digital risks.

Institutional Resilience and State Capacity in Maintaining Macroeconomic Stability in the Digital Economy Era Towards Golden Indonesia 2045

Institutional resilience and state capacity are fundamental to maintaining macroeconomic stability in the digital-economy era, characterized by accelerated technological transformation, global market integration, and the increasing complexity of digital financial risks. From the perspective of modern rule of law theory, the state no longer functions merely as a passive regulator but must instead act as an institution with effective regulatory, administrative, technological, supervisory, and crisis response capacity. The Indonesian Constitution, through Article 23D of the 1945 Constitution of the Republic of Indonesia, affirms that the state has a central bank whose structure, position, authority, responsibilities, and independence are regulated by law as part of the national economic governance system. This provision is further elaborated in Law Number 23 of 1999 concerning Bank Indonesia, as most recently amended by Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector, specifically Articles 7 and 8, which assign Bank Indonesia the task of maintaining the stability of the rupiah and the stability of the national payment system. In the context of the digital economy, this function is no longer defined as controlling inflation and maintaining conventional monetary stability, but must be expanded to include strengthening the resilience of the national digital financial system. Empirically, the public's increasing dependence on mobile banking, e-wallets, QRIS (Qualifying Transactions), and digital transactions has made national economic stability highly dependent on the resilience of digital infrastructure and the state's ability to manage financial technology risks. Disruptions to digital payment systems, cyber-attacks on financial institutions, or customer data leaks can quickly lead to a crisis of public trust, which can have systemic impacts on national economic stability.

The state's institutional resilience in maintaining macroeconomic stability is also largely determined by the ability to effectively coordinate between financial and digital supervisory institutions. In the Indonesian legal system, financial sector supervisory authority is distributed among various state institutions, including Bank Indonesia (Bank Indonesia Law), the Financial Services Authority (OJK) (Law No. 21 of 2011 concerning the Financial Services Authority), the Ministry of Finance, the Ministry of Communication and

Digital (Kominfo), the National Cyber and Crypto Agency (Badan Cyber dan Encryption) (Presidential Regulation No. 53 of 2017), and the Financial System Stability Committee (Law No. 9 of 2016 concerning the Prevention and Management of Financial System Crises). Article 39 of Law Number 9 of 2016 established the Financial System Stability Committee (KSSK) as a coordination forum to maintain the stability of the national financial system. However, empirically, this coordination still faces various structural obstacles, such as sectoral egos, slow data exchange, overlapping authorities, and limited interoperability of digital supervisory systems. In several cases of illegal online lending and public financial data leaks, handling is often partial because each institution operates based on sectoral authority without an adequate national supervisory integration system. This situation indicates that Indonesia's capacity to address digital economic threats still faces serious institutional challenges, particularly in building integrated digital governance that can simultaneously link monetary supervision, cybersecurity, data protection, and financial system stability.

In addition to institutional coordination issues, state capacity is also being tested by increasing global geopolitical threats and economic cyberwarfare, which impact national macroeconomic stability. In the digital era, economic warfare is no longer solely waged through trade embargoes or manipulation of conventional financial markets, but also through cyberattacks on the country's strategic infrastructure, control of national economic data, manipulation of digital algorithms, and dominance of global technology platforms. Empirically, various countries are beginning to face the threat of cyberattacks against central banks, national payment systems, and digital financial infrastructure, which may paralyze economic activity broadly. Indonesia itself faces similar risks due to the high level of digitalization of its payment system and increasing dependence on foreign technology. Although Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, prohibits illegal access through Article 30 and manipulation of electronic systems through Article 32, these regulations are still oriented towards general cybercrime and do not specifically establish a national digital economic defense system.

From the perspective of state capacity theory, this situation demonstrates that a country's ability to maintain economic stability is determined not only by fiscal and monetary strength but also by its ability to build cyber resilience and national technological sovereignty.

The development of central bank digital currencies (CBDCs) and the transformation of the international financial architecture also pose new challenges to state institutional resilience. Many countries have begun developing central bank digital currencies in response to the increasing use of cryptocurrencies and the dominance of global technology companies in the international payment system. Indonesia, through Bank Indonesia, has developed the Digital Rupiah project as part of the transformation of its national payment system and strengthening of digital monetary sovereignty. Legally, Bank Indonesia's authority in the payment system is regulated by Article 8(b) of the Bank Indonesia Law, but regulations related to digital currencies and cross-border integration are still in their

infancy. Empirically, the transformation of the digital-based global payment system poses new risks in the form of capital flow volatility, dependence on foreign platforms, and the potential for reduced state control over cross-border digital transaction flows. Furthermore, the development of stablecoins and global cryptocurrencies could also impact the effectiveness of national monetary policy if not balanced by strengthening state regulations and oversight capacity. Therefore, Indonesia's institutional resilience must be directed at safeguarding its digital economic sovereignty while maintaining national macroeconomic stability amidst changes in the global financial architecture.

From the perspective of institutional resilience theory, macroeconomic stability in the digital era depends heavily on the country's ability to build institutions that are adaptive, responsive, and resilient to technological change and global dynamics. Institutional resilience is not only related to the existence of formal institutions but also concerns their ability to detect risks, respond quickly to threats, build public legitimacy, and maintain public trust in the national economic system. In the Indonesian context, empirical issues such as the prevalence of financial data leaks, the high number of illegal online lending cases, ransomware attacks on public institutions, and the public's weak digital literacy demonstrate that the country's institutional resilience still faces serious challenges. Although Law Number 27 of 2022 concerning Personal Data Protection regulates the obligation to protect personal data through Article 35 and administrative sanctions through Article 46, the implementation of oversight and law enforcement remains suboptimal. As a result, the public remains vulnerable to data exploitation and digital financial crimes, which can undermine public trust in the national economic system. In the concept of good financial governance, public legitimacy is a key factor in a country's success in maintaining economic stability. Therefore, strengthening state capacity must be achieved not only through regulatory reform, but also through strengthened governance, integrated oversight, and the development of a national digital security culture.

Strengthening institutional resilience and state capacity is a key prerequisite for maintaining macroeconomic stability toward Golden Indonesia 2045. The state must be able to build an integrated, adaptive, and technology-based digital economic oversight system to address the increasingly complex threat of global economic disruption. In a legal context, institutional reforms need to be directed at strengthening inter-institutional coordination, integrating a national early warning system, developing cyber financial governance, and establishing a rapid and effective digital crisis response mechanism. The provisions of Article 33, paragraph (4) of the 1945 Constitution of the Republic of Indonesia, which affirms the principles of economic democracy with the principles of togetherness, efficiency with justice, sustainability, and independence, must be interpreted progressively in the context of modern digital economic transformation. Therefore, the country's capacity is no longer measured solely by its ability to create regulations, but also by its ability to maintain digital economic stability, protect national data and financial infrastructure, and maintain Indonesia's economic sovereignty amidst technology-based global competition towards the realization of Golden Indonesia 2045.

Legal Reformulation of Digital Risk-Based Financial System Stability Supervision as an Effort to Strengthen State Capacity Towards Indonesia Emas 2045

Legal reformulation of digital risk-based financial system stability supervision must begin with a shift in the legal paradigm from a conventional sectoral supervision model to an integrated digital financial supervision model based on technology, data integration, and digital systemic risk mitigation. Indonesia's current financial supervision legal system remains fragmented between the authorities of Bank Indonesia, the Financial Services Authority (OJK), the Ministry of Finance, the Ministry of Communication and Digital, and the National Cyber and Crypto Agency (BSSN), resulting in partial oversight of digital threats and an unresponsive response to the dynamics of financial technology. Therefore, a reformulation of Law Number 9 of 2016 concerning the Prevention and Management of Financial System Crises is needed by adding norms regarding digital financial crises and systemic digital financial risk as part of the threat to national financial system stability. A concrete action that needs to be taken is the establishment of a National Digital Financial Supervision Integration Center under the coordination of the Financial System Stability Committee (KSSK), which functions to integrate real-time supervisory data from Bank Indonesia, the Financial Services Authority (OJK), Komdigi, BSSN, PPATK, and other financial institutions.

Strengthening the legal basis for this data integration can be achieved through amendments to Articles 39 and 44 of Law Number 9 of 2016, but the reform should not transform KSSK into a new sectoral regulator or diminish the institutional independence of Bank Indonesia and the Financial Services Authority. KSSK should instead exercise coordinating, systemic risk assessment, crisis escalation, and joint-response authority in relation to cross-sectoral digital financial threats.

Under this model, Bank Indonesia would retain its statutory authority over monetary stability and payment systems; OJK would retain regulatory and supervisory authority over financial services institutions; the Ministry of Finance would retain fiscal and financial-policy responsibilities; BSSN would provide national cybersecurity coordination and technical threat analysis; the Ministry responsible for communication and digital affairs would retain authority concerning electronic systems and digital infrastructure; and PPATK would continue exercising its statutory authority concerning financial intelligence. KSSK would function as the legally designated forum for integrating systemic risk information and coordinating responses when a threat exceeds the jurisdiction or operational capacity of a single institution.

Accordingly, KSSK's strengthened authority should be limited to requiring legally authorized information sharing, convening joint assessments, determining crisis escalation levels, recommending coordinated measures, and activating a Digital Financial Crisis Protocol. Individual regulatory, investigative, monetary, or supervisory decisions must remain within the statutory authority of the relevant institution.

In addition to integrated supervision, legal reformulation must also be directed at developing cyberfinancial governance as part of the national economic defense system. Currently, financial sector cybersecurity regulations are scattered across various general

regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024 and Law Number 27 of 2022 concerning Personal Data Protection. However, there is no specific regulation regarding the cyber resilience of the national financial sector. Therefore, the establishment of a Financial Sector Cyber Resilience Law that regulates national digital security standards, cyber resilience obligations for financial institutions, systemic cyberattack mitigation, and emergency response mechanisms for cyberfinancial attacks. Concrete actions that must be taken include mandatory periodic cybersecurity audits for all financial services institutions, the establishment of a National Financial Cyber Security Center integrated with the National Cyber and Crypto Agency (BSSN), and the implementation of mandatory cyber incident reporting for banks, fintech companies, and digital payment system providers. Furthermore, the government needs to establish a national simulation system for handling regular financial cyber crises to improve the response capacity of state institutions to digital threats. Thus, financial system stability will no longer be viewed solely from a monetary economic perspective, but also as part of technology-based national security.

Subsequent legal reforms must be directed at establishing a digital crisis management framework capable of anticipating the fast-moving, cross-sectoral, and cross-border nature of digital crises. The current legal framework for crisis management still focuses primarily on conventional financial crises, while digital threats may develop rapidly through interconnected payment infrastructure, social-media-driven panic, cyberattacks, or failures of algorithmic financial systems. Therefore, a Digital Financial Crisis Protocol should be incorporated into the legal framework governing the prevention and management of financial system crises.

The proposed National Digital Financial Early Warning System should use artificial intelligence as an analytical and detection tool rather than as an autonomous decision-maker. Relevant indicators may include abnormal transaction concentration, simultaneous disruption across payment infrastructures, unusual liquidity withdrawal patterns, large-scale cybersecurity incidents affecting critical financial infrastructure, coordinated dissemination of demonstrably false financial information, and abnormal market movements that exceed predetermined risk parameters. An alert should not automatically constitute a systemic financial threat merely because one indicator is detected.

The system should apply a tiered validation mechanism consisting of automated detection, technical verification, cross-institutional confirmation, and human review by authorized officials. Thresholds should be periodically determined and reviewed based on the size, interconnectedness, speed of propagation, affected institutions, and potential impact of the incident. Only after human validation and documented risk assessment may an alert be classified as requiring coordinated systemic intervention. Every AI-generated alert should therefore be explainable, auditable, and subject to correction where the underlying data or analytical result is inaccurate.

Extraordinary intervention under the Digital Financial Crisis Protocol, including temporary restrictions on particular digital transactions or emergency intervention in payment infrastructure, must be treated as an exceptional measure rather than an ordinary

supervisory instrument. Such intervention should only be activated where there is a documented and verified indication of an imminent or ongoing systemic threat that cannot reasonably be managed through ordinary regulatory measures.

The decision should be based on a written risk assessment, authorization through the legally designated crisis mechanism, and consultation with the institution holding primary authority over the affected sector. The intervention must satisfy the principles of legality, necessity, proportionality, limited duration, and reversibility. Any restriction should be narrowly tailored to the affected transaction, institution, infrastructure, or geographical scope and should be subject to periodic review.

The legal framework should also require documentation of the factual and legal basis for intervention, public communication to the extent compatible with crisis management, post-intervention accountability, and an ex post review mechanism. Emergency powers must automatically expire unless renewed on the basis of a new documented assessment, thereby preventing extraordinary digital crisis powers from becoming indefinite administrative authority.

Furthermore, the reformulation of the law on financial system stability supervision must also strengthen adaptive regulation and the national regulatory sandbox to address the highly dynamic developments in financial technology. Indonesia's financial sector regulations have tended to be rigid and slow to respond to technological innovation, often resulting in legal gaps in the supervision of fintech, crypto assets, artificial intelligence finance, and embedded finance. Therefore, a shift in the regulatory approach is needed from rule-based regulation to principle-based regulation, which is more flexible and adaptive to technological changes. A concrete action that can be taken is the establishment of an integrated National Digital Financial Regulatory Sandbox involving Bank Indonesia, the Financial Services Authority (OJK), and Komdigi (Ministry of Communication and Digital) to test the security, stability, and economic impact of financial technology innovations before their widespread implementation. Furthermore, the government needs to draft an omnibus regulation on the digital economy and financial system stability that harmonizes various cross-sectoral regulations to prevent overlapping authority and legal gaps. With this adaptive regulatory approach, the country can maintain a balance between technological innovation, consumer protection, and the stability of the national financial system.

Legal reform must also be directed at strengthening financial data protection and national economic data sovereignty as part of macroeconomic stability. In the digital economy era, financial data is a strategic national asset that can influence economic policy, market stability, and even national security. However, empirically, Indonesia still faces high cases of customer data leaks, misuse of online lending data, and the dominance of global technology platforms in controlling public transaction data. Therefore, it is necessary to strengthen the implementation of Law Number 27 of 2022 concerning Personal Data Protection through the establishment of a Financial Data Protection Authority with specific authority to oversee national financial data protection. Other concrete actions include mandating the storage of strategic financial data in a national data center, limiting cross-

border financial data transfers, and implementing a sovereign financial cloud for national strategic financial services institutions. Furthermore, the country needs to develop a secure and integrated national digital identity system to mitigate the risk of data theft and digital financial fraud. Strengthening financial data protection is crucial for maintaining public trust in the national digital economic system.

Legal reformulation of financial system stability oversight based on digital risk must be directed at building the capacity of a modern, resilient, adaptive, and digitally sovereign state, moving towards a Golden Indonesia 2045. Legal reform must not stop at the creation of administrative regulations, but must also create a national oversight system that integrates the financial sector, cybersecurity, data protection, and digital technology oversight. In this context, Article 33, paragraph (4) of the 1945 Constitution of the Republic of Indonesia, which affirms the principles of economic democracy based on efficiency with justice, sustainability, and independence, must be interpreted as the constitutional basis for developing national digital economic resilience. Concrete actions that the state must take include the development of a Grand Design for National Digital Economic Resilience 2045, the establishment of a National Digital Economic Stability Coordinating Agency, increasing the capacity of digital oversight human resources, and strengthening international cooperation in monitoring cross-border digital financial transactions and crimes. With this progressive and responsive legal reformulation, Indonesia will have a financial stability legal system capable of facing the threat of the global digital crisis while strengthening the country's capacity to maintain macroeconomic stability towards the realization of Golden Indonesia 2045.

Conclusion

The study shows that the digital economic transformation has changed the structure and nature of risks in the national financial system, making the legal framework for supervising financial system stability in Indonesia no longer adequate if it relies solely on conventional supervisory paradigms. The development of fintech, digital banks, artificial intelligence, crypto assets, and electronic payment systems has given rise to various forms of systemic digital risks, such as cyberattacks, digital bank runs, financial data leaks, digital shadow banking, and the dominance of global technology platforms that have the potential to disrupt national macroeconomic stability. In practice, the Indonesian legal system still faces various weaknesses, including fragmented authority among state institutions, weak coordination of digital supervision, limited cyber resilience regulation, suboptimal financial data protection, and the absence of an integrated legal framework for digital financial crisis management. It indicates that the state's capacity to face digital economic disruption is still not fully adaptive to technological change and global threats. Therefore, strengthening institutional resilience through legal reformulation of financial system stability supervision based on digital risk is an urgent need to build integrated digital financial supervision, strengthen cyber financial governance, enhance inter-institutional coordination, and create a supervisory system that is responsive, anticipatory, and resilient to digital crisis threats in order to maintain macroeconomic stability towards Indonesia Emas 2045.

This research recommends that the government and lawmakers comprehensively reformulate the legal system for financial system stability supervision by establishing integrated regulations on digital risk supervision and national digital economic resilience. This reform should be realized through a revision of Law Number 9 of 2016 concerning the Prevention and Management of Financial System Crises to include regulations on systemic digital financial risk, a digital crisis management framework, and strengthening the coordinating authority of the Financial System Stability Committee in national digital supervision. Furthermore, the government needs to establish a national digital financial supervision integration center that connects Bank Indonesia, the Financial Services Authority (OJK), the Ministry of Finance, Komdigi, BSSN, PPATK, and other relevant institutions in real time through an artificial intelligence-based early warning system. The government also needs to develop specific regulations regarding cyber financial governance, strengthen national financial data protection, establish a national regulatory sandbox that is adaptive to financial technology innovation, and improve human resource capacity and national digital oversight infrastructure. Moreover, strengthening international cooperation in the supervision of cross-border digital transactions, economic cybersecurity, and global digital asset control is necessary to safeguard national economic sovereignty amidst the transformation of the global financial architecture. With these steps, Indonesia is expected to be able to build a modern, adaptive legal system for financial stability, oriented towards strengthening the state's capacity to achieve macroeconomic stability and the vision of Indonesia Emas 2045.

References

- Abrini, R. P., & Paraya, E. P. (2020). Fungsi pengawasan oleh lembaga Otoritas Jasa Keuangan terhadap sektor perasuransian ditinjau dari hukum pengawasan. *Buletin Hukum Kebanksentralan*, 27–38.
- Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politika Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*.
- Asiyanti, A. P., & Agussalim, A. (2024). Strategi Manajemen Risiko dan Keamanan Siber dalam Ekonomi Digital: Tinjauan Literatur. *Jurnal Penelitian Sistem Informasi (JPSI)*.
- Azizah, H. A. (2025). Regulasi Dan Pengawasan Perbankan Oleh Otoritas Jasa Keuangan (OJK). *Menulis: Jurnal Penelitian Nusantara*, 481–461.
- Dzikri, I. (2016). Negara dan Kapasitas Adopsi Inovasi: Studi Kasus Transformasi Pertahanan Indonesia Periode 1998-2014. *Global: Jurnal Politik Internasional*, 131–151.
- Fitrianto, B. R. (2025). Urgensi Pengaturan Cyber Insurance (Asuransi Siber) Wajib Bagi Bank. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 3922–3935.
- Gunibala, Z. Y. (2025). Dampak Finansial Serangan Siber Terhadap Kinerja Korporasi: Scoping Review. *Jurnal Daya Saing*, 493–501.
- Parulian, S. D. (2021). Studi tentang ancaman dan solusi serangan siber di indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT)*, 85–92.
- Purba, D. S. (2024). Peran Bank Sentral terhadap stabilitas sistem keuangan. *Jurnal PenKoMi*:

- Kajian Pendidikan Dan Ekonomi*, 380–391.
- Rahakbauw, I. (2024). Analisis Potensi Ancaman Siber pada Bidang Ekonomi di Indonesia. *Jurnal Kajian Strategik Ketahanan Nasional*.
- Rahayu, N., Supriyono, I. A., Mulyawan, E., Nurfadhillah, F., Yulianto, D. R., Ramadhan, A. Z. (2023). Pembangunan Ekonomi Indonesia Dengan Tantangan Transformasi Digital. *ADI Bisnis Digital Interdisiplin (ABDI Jurnal)*, 1–4.
- Satria, M., & Handoyo, S. (2022). Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. *Journal de Facto*, 1–12.
- Simbolon, M. M., Kesuma, I. G., & Wibowo, A. E. (2021). Kejahatan Siber pada Penyelenggaraan Perdagangan Berbasis Sistem Elektronik Dalam langkah Pengamanan Pertumbuhan Ekonomi Digital Indonesia. *Defendonesia*, 1–12.
- Sinaga, Z. A. (2025). Transformasi Ekonomi Indonesia Menuju Ekonomi Digital: Tantangan Dan Strategi. *Jurnal Rumpun Manajemen Dan Ekonomi*, 26–33.
- Sjofjan, L., Al-Fikri, M. F., Farisqi, M. R., Atha, M., & Saputra, F. (2025). Urgensi Penguatan Regulasi Perbankan Dalam Menjaga Stabilitas Sistem Keuangan Nasional. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, 2152–2158.
- Sudiantini, D., Ayu, M. P., Aswan, M. C., Prastuti, M. A., & Apriliya, M. (2023). Transformasi digital: Dampak, tantangan, dan peluang untuk pertumbuhan ekonomi digital. *Trending: Jurnal Manajemen Dan Ekonomi*, 21–30.
- Syah, E., Weharima, H., Susilo, T., Basuki, T., & Akad, A. M. (2025). Serangan Siber terhadap Infrastruktur Kritis: Ancaman Bagi Keamanan dan Kesejahteraan Masyarakat. *JURNAL SYNTAX IMPERATIF: Jurnal Ilmu Sosial Dan Pendidikan*, 145–154.
- Widyasari, R., & Hermawan, A. (2024). Ekonomi Digital: Peluang dan Tantangan Dalam Transformasi Ekonomi Nasional. *Journal Central Publisher*, 2758–2763.