Technology in Society 81 (2025) 102838

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Algorithmic trust and regulation: Governance, ethics, legal, and social implications blueprint for Indonesia's central banking

Arif Perdana [a,*], Saru Arifin [b], Novi Quadrianto [c]

[a] Monash University, Indonesia
[b] Universitas Negeri Semarang, Indonesia
[c] University of Sussex, UK

ARTICLE INFO

Keywords:
Algorithm-driven systems
GELSI framework
Ethical concerns
Data governance
Indonesia

ABSTRACT

Algorithm-driven financial systems significantly influence monetary stability and payment transactions. While these systems bring opportunities like automation and predictive analytics, they also raise ethical concerns, particularly biases embedded in historical data. Recognizing the critical role of governance, ethics, legal considerations, and social implications (GELSI), this study introduces a framework tailored for algorithmic systems in financial services, focusing on Indonesia's evolving regulatory environment. Using the Multiple Streams Approach (MSA) as our theoretical lens, we offer a framework that augments existing quantitative methodologies. Our study provides a nuanced, qualitative perspective on algorithmic trust and regulation. We proffer actionable strategies for the Central Bank of Indonesia (BI), emphasizing stringent data governance, system resilience, and cross-sector collaboration. Our findings highlight the critical importance of ethical guidelines and robust governmental policies in mitigating algorithmic risks. We combine theory and practical advice to show how to align problems, policies, and politics to create practical opportunities for algorithmic governance. This study contributes to the evolving discourse on responsible financial technology. Our study recommends a balanced way to manage the challenges of innovation, regulation, and ethics in the age of algorithms.

1. Introduction

As a key component of modern financial services, algorithm-driven systems play a crucial role in shaping payment systems and maintaining monetary stability. They fundamentally alter financial transactions and influence the overall stability of the monetary environment. These systems are gradually transforming financial services, offering various advantages, such as automation, credit scoring, predictive analytics, and enhanced customer experience (Gomber et al., 2018). The integration of advanced algorithms and sophisticated data analytics, however, introduces both opportunities and challenges that require careful evaluation.

Despite the benefits of algorithmic systems in accelerating financial services, recent research has highlighted various ethical and social concerns associated with their widespread adoption (Carlsson & Rönnblom, 2022; Coeckelbergh, 2018). The rise of digital transformation has intensified moral considerations (Belenguer, 2022). These systems are trained on historical datasets, which may contain biased patterns reflecting past discriminatory practices. Their functionality relies on accurate data inputs and algorithmic processes; however, inherent biases or inaccuracies can distort outcomes. When influenced by bias, algorithmic systems can result in discriminatory behavior, exclusion, or unequal performance, ultimately undermining public trust in the financial sector (Akter et al., 2021).

Effectively managing potential technological risks requires both technical and non-technical approaches, including legal considerations, to enhance the role of financial authorities in anticipating and mitigating these risks. To address this challenge, we propose the Governance, Ethics, Legal, and Social Implications (GELSI) framework for financial algorithmic systems. This study is guided by the following research question: *How can the risks associated with algorithmic systems in financial services be effectively mitigated through the GELSI framework?*

To explore this, we apply the Multiple Streams Approach (MSA) as a valuable lens for understanding the implementation of responsible algorithmic system frameworks (Hoefer, 2022; Kingdon, 2003; Olszowski, 2024). The MSA conceptualizes policymaking as the convergence of problem, policy, and political streams at critical junctures. The problem stream addresses issues such as bias and transparency in

* Corresponding author.
E-mail addresses: Arif.Perdana@monash.edu (A. Perdana), saruarifin@mail.unnes.ac.id (S. Arifin), N.Quadrianto@sussex.ac.uk (N. Quadrianto).

https://doi.org/10.1016/j.techsoc.2025.102838
Received 3 December 2023; Received in revised form 9 February 2025; Accepted 9 February 2025
Available online 11 February 2025

algorithmic governance, while the policy stream focuses on developing technical standards and regulatory frameworks. The political stream encompasses public opinion and interest group advocacy. By aligning these streams, policymakers can create opportunities for meaningful governance, enabling them to tackle complex challenges of algorithmic financial systems effectively.

This study examines Bank Indonesia (BI) as the central authority responsible for maintaining monetary and financial stability while integrating algorithmic systems into its regulatory framework. As the financial sector rapidly evolves, BI must balance innovation with risk mitigation, particularly in data governance and cybersecurity. Although recent legislative advancements in personal data protection enacted in 2022 have strengthened regulatory efforts, challenges persist in leveraging data to develop and implement responsible algorithmic mechanisms in finance.

To address these challenges, we developed the GELSI framework through qualitative inquiry (Myers, 2013), conducting in-depth interviews with 18 experts from finance, technology, and law. These experts were categorized into two groups: academics (including specialists in law, information technology/IT, and data science) and practitioners (comprising finance professionals, IT experts, and bankers). Their insights shed light on BI's role in algorithmic adoption. Using thematic analysis and the Analytical Hierarchy Process (AHP) (Tavana et al., 2023), our study identified key dimensions essential for ethical and responsible algorithmic governance.

Findings from the GELSI framework highlight the importance of data governance, ethical guidelines, legal protections, and cross-sector collaboration. Data governance is crucial, requiring well-defined policies, structured classification systems, and regular security updates to mitigate cyber threats. Ethical guidelines play a key role in reducing bias and enhancing transparency, thereby fostering trust in algorithmic decision-making. Additionally, education, and digital literacy initiatives are essential for raising awareness and promoting the responsible adoption of algorithmic systems. To ensure fairness in financial decision-making, legal assistance should be available to economically vulnerable individuals affected by algorithmic biases. Collaboration through memoranda of understanding (MOUs) can facilitate the development of standardized regulatory frameworks among financial institutions. Furthermore, robust government policies must strike a balance between technological innovation and regulatory mandates to maintain systemic stability and security. The GELSI framework builds on MSA and complements quantitative models such as Sustainability, Accuracy, Fairness, and Explainability (SAFE) (Babaei et al., 2025; Giudici & Raffinetti, 2023) and IBM's Fairness 360 Toolkit.[1] We propose actionable strategies for BI, including enhanced data governance protocols, strengthened system resilience, rigorous algorithmic evaluation, and improved cross-sector cooperation. These recommendations aim to provide a comprehensive approach to managing algorithmic risks in Indonesia's financial sector.

This paper is structured as follows: Section 2 reviews BI's role in financial governance, Section 3 outlines the research methodology, Section 4 presents findings categorized under the GELSI dimensions, Section 5 discusses the framework's implications, Section 6 highlights theoretical and practical contributions, and Section 7 concludes with key insights and directions for future research.

2. Literature review

As companies explore the potential of technology, four critical GELSI dimensions have become increasingly important (Ghioni et al., 2023). Organizations must make significant decisions to ensure that new technologies are developed, deployed, and utilized responsibly and sustainably, allowing users to maximize benefits while minimizing negative impacts. Addressing these concerns early in the development process enables stakeholders to ensure that emerging technologies align with societal needs (Theodorou & Dignum, 2020). Governance systems play a crucial role in managing the responsible and transparent development and deployment of new technologies, ensuring alignment with societal expectations (Buhmann & Fieseler, 2021). Ethics remain central to all decision-making (Dubber et al., 2020; Strasser, 2022), guiding appropriateness based on specific values and defining the expected behavior of individuals (Powers et al., 2020). Organizations must uphold ethical standards despite the challenges they face (Holford, 2022). Maintaining strong ethical principles can also provide a competitive advantage in a market where reputation and values are crucial. Additionally, the legal implications of new technologies must be carefully assessed to ensure compliance with relevant laws, regulations, and standards (Dignum, 2019). Social considerations encompass the broader impact of new technologies on social structures, economic systems, and cultural norms (Ghioni et al., 2023).

While previous studies have explored GELSI-related dimensions in algorithmic systems and proposed guidelines, these guidelines primarily address the general application of such systems (Floridi, 2021; Ghioni et al., 2023; Powers et al., 2020; Theodorou & Dignum, 2020). Given the inherently high risk and restrictive conditions in the financial sector, the use of algorithmic systems must be examined explicitly. Failure to manage financial risks effectively can have severe consequences for both individuals and society (Bussmann et al., 2020; Svetlova, 2022).

2.1. Bank Indonesia's role and challenges in the era of algorithmic financial systems

BI and the Financial Services Authority (OJK) are two key institutions in Indonesia's financial landscape, each with distinct yet complementary functions,[2,3,4] As the central bank, the BI is primarily responsible for formulating monetary policy, maintaining payment system stability, and implementing macroprudential regulation to ensure overall financial system stability and sustainable economic growth. To achieve these goals, BI utilizes tools such as interest rate management, currency exchange regulation, and liquidity control. In contrast, OJK, an independent state agency, focuses on microprudential regulation and the supervision of the financial services sector, including banks, capital markets, insurance, and other non-banking financial entities. Its primary goal is to ensure the orderly, fair, and transparent operation of financial sector activities, contributing to a stable and sustainable financial system while protecting consumer and public interests. Coordination between BI and OJK is crucial for maintaining comprehensive financial stability. BI provides macroprudential insights, while OJK offers microprudential oversight. Their collaboration allows for the effective management of systemic risks and promotes the health of the financial sector, including emerging areas such as data and algorithmic governance.

Various perspectives and challenges arise from integrating algorithmic systems into financial services (Bussmann et al., 2020; Svetlova, 2022; Zhou et al., 2022). When used properly, these systems can help organizations achieve unprecedented levels of efficiency, accuracy, and intelligence (Polak et al., 2020; Zhou et al., 2022). The development of this technology has, however, also introduced new vulnerabilities that must be carefully understood and promptly addressed (Svetlova, 2022). BI is at the forefront of Indonesia's monetary and financial system. With its mandate grounded in the BI Act, BI works diligently to ensure the

[1] https://aif360.res.ibm.com/.

[2] https://ojk.go.id/en/kanal/perbankan/stabilitas-sistem-keuangan/Pages/Peran-Bank-Indonesia.aspx.

[3] https://www.bi.go.id/en/fungsi-utama/stabilitas-sistem-keuangan/koordinasi-bi-lainnya/default.aspx.

[4] https://ojk.go.id/id/kanal/perbankan/ikhtisar-perbankan/Pages/Peraturan-dan-Pengawasan-Perbankan.aspx.

stability of the rupiah, a robust payment system, and overall economic system stability.[5] Algorithmic systems have the potential to enhance central banks' operating models, particularly in identifying data anomalies, making reliable macroeconomic projections, and leveraging unstructured data (Jacobs, 2023; Mirestean et al., 2021). As technology, including algorithmic systems, becomes increasingly integral to the financial sector, the role of central banks—BI included—in risk mitigation is crucial (Mirestean et al., 2021). Maintaining the stability of the rupiah in terms of inflation and exchange rates is essential to Indonesia's economic prosperity. BI prioritizes inflation control as a key objective by adopting an inflation-targeting framework (ITF).[6] Stable inflation and exchange rates are indicators of a robust economy, which is vital for sustainable growth. Importantly, any technological advancement, including algorithmic systems, that could disrupt this stability requires rigorous supervision.

After the 2008 Global Financial Crisis, the world became acutely aware of the domino effect that a destabilized financial system can have on the broader economy.[7] For BI, ensuring financial system stability involves enabling efficient functioning, promoting resilience against shocks, and ensuring that the system contributes positively to national economic growth.[8] While algorithmic systems can optimize many financial processes, unchecked systems or biased algorithms can introduce unforeseen risks that may jeopardize system stability (Leitner et al., 2024; Svetlova, 2022). Historically, payment systems have been essential for ensuring smooth economic activity. From authorization to clearing and settlement, each step is crucial.[9] As digital transactions have become the norm, algorithmic systems are frequently employed to expedite processes and detect fraudulent activities. However, these systems also introduce a layer of complexity, potentially making the system vulnerable if not adequately managed or regulated.

2.2. Multiple Streams Approach for algorithmic systems Framework Implementation

The MSA offers a framework for implementing responsible algorithmic systems by aligning three independent streams—problems, policies, and politics—at critical junctures to create policy windows for change (Béland & Howlett, 2016; Kingdon, 2003; Olszowski, 2024). Applying MSA to responsible algorithmic systems emphasizes strategies for integrating these streams to drive policy action (Olszowski, 2024).

In the problem stream, algorithmic systems raise concerns related to bias, transparency, privacy, and job displacement. However, defining these as issues requiring government intervention depends on framing strategies (Hoefer, 2022). Policy advocates must emphasize concrete risks, such as algorithmic failures, to position these concerns as urgent public safety threats. High-profile controversies can serve as 'focusing events' that elevate the issue on the policy agenda (Béland & Howlett, 2016). Advocates should also link algorithmic system risks to broader policy issues, such as fairness and economic security, to build consensus for regulatory intervention.

The policy stream consists of technical standards, ethical guidelines, regulatory frameworks, and governance models for responsible algorithmic systems (Cairney & Jones, 2016). Policies undergo a 'softening up' process, where they are refined for feasibility and acceptability before adoption. Advancing responsible algorithmic governance requires well-defined, evidence-backed proposals that align with political and practical constraints. This includes piloting initiatives, demonstrating their effectiveness, and translating technical concepts into actionable policies (Jones et al., 2016). Policy entrepreneurs play a crucial role in championing viable approaches.

The political stream encompasses public opinion, interest group advocacy, and government changes (Olszowski, 2024; Zahariadis, 2016). For responsible algorithmic system policies to gain traction, they must align with prevailing political priorities. Advocates can frame governance as a matter of national competitiveness, public safety, or economic fairness to appeal to policymakers. Broad coalitions across industries, civil society, and governments are essential to mobilizing support (Khanal et al., 2024). Public concerns over algorithmic risks can also create pressure for policy action.

MSA suggests that policy change occurs when these three streams converge, creating a policy window (Cairney & Jones, 2016; Jones et al., 2016). For responsible algorithmic governance, this could occur after a major controversy or through a gradual shift in concerns. When a window opens, policy entrepreneurs must be ready to connect well-defined problems with feasible solutions that align with the political climate (Hoefer, 2022). This requires having policy proposals prepared to capitalize on emerging opportunities. Given the rapid evolution of algorithmic systems, flexibility in policy development is essential.

While MSA was developed for U.S. policymaking, it has been applied in comparative contexts (Cairney & Jones, 2016). Institutional differences affect how these streams interact. In centralized systems, advocacy may focus on key decision-makers, while broader coalitions may be necessary in decentralized systems. International coordination is also crucial, as algorithmic system governance transcends national borders. The European Union's AI Act may, for example, create external pressure for policy adoption in other regions (Béland & Howlett, 2016). Furthermore, large technology firms are playing an increasingly global role in shaping policy streams by influencing problem definitions, promoting preferred solutions, and leveraging political power (Khanal et al., 2024).

MSA offers valuable insights for responsible algorithmic system governance. By strategically aligning problem definitions, policy solutions, and political momentum, advocates can create opportunities for meaningful regulation (Jones et al., 2016; Zahariadis, 2016). However, challenges persist, for example, policy windows can close quickly, and competing definitions or solutions may take precedence (Hoefer, 2022). The fast-changing nature of algorithmic systems further complicates policymaking. To seize policy windows, sustained efforts are required to elevate concerns, refine governance strategies, and build political support.

2.3. The pillar of governance in algorithmic systems

Organizations have traditionally used algorithmic systems to support human decision-making, but fully automated decisions can compromise individual autonomy and privacy, potentially leading to financial or physical harm. Regulations such as the UK's General Data Protection Regulation (GDPR) prohibit companies from making significant decisions solely through automation[10]. The rise of algorithmic systems has fostered interdisciplinary collaboration, bringing ethical and societal considerations to the forefront (Floridi, 2021). These systems differ from other emerging technologies due to their hidden infrastructure, anthropomorphic elements, interdependent stakeholders, and various technical and societal risks (Xue & Pang, 2022). Evaluating their benefits requires careful attention to these complexities (Morley et al., 2020; Munoko et al., 2020; Wirtz et al., 2022).

Governance is crucial for ensuring the responsible development, use, and management of algorithmic systems (Gordon et al., 2022). Effective

[5] https://www.bi.go.id/en/fungsi-utama/default.aspx.
[6] https://www.bi.go.id/en/fungsi-utama/moneter/Default.aspx.
[7] https://www.weforum.org/agenda/2018/10/lasting-effects-the-global-economic-recovery-10-years-after-the-crisis/.
[8] https://www.bi.go.id/en/fungsi-utama/stabilitas-sistem-keuangan/ikhtisar/Default.aspx.
[9] https://www.bi.go.id/en/fungsi-utama/sistem-pembayaran/default.aspx.
[10] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/.

governance includes policies, procedures, and standards that uphold integrity, security, and fairness (Kuziemski & Misuraca, 2020; Wirtz et al., 2022). Ethical concerns can be addressed through robust data governance strategies that ensure data quality, security, and usability throughout its lifecycle (Bollweg, 2022; Mahanti, 2021). Governance frameworks must make data accessible and understandable while mitigating ethical risks (Palladino, 2022).

Cyber risk management in algorithmic systems has become a key research focus, viewed from different perspectives. Aldasoro et al. (2022) emphasized the role of strong cybersecurity practices in safeguarding data integrity and availability. Hałaj et al. (2024) examined financial stability through a systemic lens, highlighting the need for holistic data management. Both studies acknowledged the impact of cloud technologies, with Aldasoro et al. (2022) noting lower cyber-event costs associated with cloud services, while Hałaj et al. (2024) warned of increasing systemic risks due to the dominance of major cloud providers. These insights underscore the intertwined benefits and risks of algorithmic system governance. BI operates at the intersection of technological and regulatory oversight, as the increasing reliance on digital and algorithmic systems heightens cyber threats (Rachman, 2023). Cyber-attacks on BI could destabilize financial markets and payment systems, directly impacting its core mandate (Heriyanto, 2023). Additionally, algorithmic-enabled trading could introduce market volatility, further reinforcing BI's role in maintaining financial stability.

BI primarily engages with algorithmic systems at the macro level (Bank Indonesia, 2023; Pusparisa, 2023), ensuring they do not disrupt the financial ecosystem. Its proactive approach is evident in the establishment of the Financial Artificial Intelligence Unit (FAIU), which collaborates with anti-money laundering systems to detect suspicious transactions (Bank Indonesia, 2023). Since data form the backbone of algorithmic systems, BI prioritizes macro-level data governance to maintain accuracy and reliability (Bank Indonesia, 2023; Bank Indonesia, 2021). Critical financial infrastructure, including the BI-Real-Time Gross Settlement (RTGS), BI clearing system, and BI-Fast, falls under its oversight. Corrupted macro data can jeopardize financial stability, making data integrity a key focus. The BI regulatory sandbox further ensures that payment innovations, including algorithmic solutions, are tested within a controlled environment before broader integration, aligning with BI's financial stability mandate.

2.4. Ethical dimensions of algorithmic systems

Three key ethical issues—privacy, bias, and accountability—are critical in managing algorithmic systems in financial services, particularly in payment systems and monetary stability (Stahl, 2021). If not adequately addressed, these systems can lead to missed opportunities, economic losses, social disadvantages, and a loss of freedom, ultimately harming businesses, individuals, and communities. Privacy risks in algorithmic systems are a major concern in financial services (Bartlett et al., 2022; Chou, 2020). These systems rely heavily on personal data, including social media activity and location information, to predict behaviors and preferences (Bartneck et al., 2021). While some data are collected with user consent, questions remain about whether individuals fully understand how their information is stored, shared, or manipulated. The rise of digitalization presents a paradox for businesses: it enables them to capture valuable customer insights but also exposes sensitive data to potential threats (King & Forder, 2016; Švarc et al., 2024). While user data can enhance product development and marketing (Perera et al., 2015), companies must prioritize data protection and confidentiality.

Bias in algorithmic systems stems from the datasets they use to make predictions and classifications (Gupta et al., 2021). Even when data quality is high, algorithms may reflect existing social biases, such as gender or ethnic discrimination, leading to unfair outcomes in hiring, credit access, or financial rankings (Akter et al., 2021; Belenguer, 2022; Hsu, 2022). Excluding sensitive attributes, such as gender or ethnicity, does not eliminate bias, as proxy variables can still reinforce patterns of discrimination (Johnson, 2021). Addressing bias requires careful monitoring and intervention to prevent the perpetuation of societal inequalities.

Accountability in algorithmic decision-making is essential to ensuring transparency and assigning responsibility (Barredo Arrieta et al., 2020; de Laat, 2018; Hind, 2019). These systems, as reflections of societal norms, require a robust accountability framework. Since algorithms lack intent or moral agency, responsibility must reside with human or legal entities (Dignum, 2019; Floridi, 2021). This creates challenges in determining accountability, particularly when unintended consequences arise. Institutions must ensure human oversight in critical decisions, such as risk assessments, and provide clear explanations for algorithmic outcomes similar to judicial reasoning (Jammalamadaka & Itapu, 2022). Regulatory bodies emphasize the importance of anthropocentric monitoring to prevent unethical decision-making.

Accountability is particularly relevant for central banks, which focus on preventing systemic risks in financial regulation (Mirestean et al., 2021). Algorithmic systems introduce potential vulnerabilities that could threaten monetary stability, a core responsibility of central banking (Daníelsson et al., 2022). As custodians of financial transactions, central banks must uphold public trust and mitigate risks associated with algorithmic decision-making, including data breaches and misuse. The integration of algorithmic systems in financial markets requires careful oversight to maintain stability and fairness (Jacobs, 2023). Latent biases in these systems could distort financial practices, raising concerns about equity and integrity. The convergence of accountability, systemic risk, and algorithmic implementation underscores the need for a comprehensive regulatory approach in the digital age. Ensuring fairness, transparency, and robust oversight in algorithmic systems is essential to maintaining public confidence and financial stability.

2.5. Legal dimension of algorithmic systems

The rapid growth of technology powered by sophisticated algorithms has raised concerns regarding the ethical, appropriate, and legal applications of these systems. Legal evaluations span from the administrative aspects of these algorithms to their potential criminal implications. Central administrative law principles, including non-discrimination, accountability, and transparency, demand stringent supervision (Fitsilis, 2019). These algorithms depend primarily on the data collected and processed by the controller. Thus, these systems must assess fairness within a robust legal framework. The safeguards enshrined in personal data protection should be embedded in algorithmic regulations to ensure individual human rights. Brazil, for instance, uses data privacy laws to strengthen non-discrimination, suggesting that impact assessments can help reduce bias in automated decision-making (Pedigoni Ponce, 2023).

Algorithmic applications, especially in sectors such as finance and recruitment, have triggered extensive research on the nature and effects of automated decision-making (Ahmed et al., 2022). As a torchbearer of regulatory prudence, BI ensures that swift advancements in algorithmic systems do not overshadow or outpace relevant regulations. Crafting a regulatory framework that evolves with technological progress is essential to avoiding potential ambiguities and legal pitfalls (Danielsson, 2023; Daníelsson et al., 2022). Moreover, a deeper examination of BI's role in algorithmic systems reveals a strong emphasis on macro-level implications. Undue reliance on algorithmic systems, particularly without necessary transparency, can introduce obstacles in decisive actions and problem-solving, especially in crisis scenarios. BI's central role in safeguarding the stability, predictability, and payment systems of Indonesia's financial fabric makes these risk vectors critically relevant. As we navigate an era dominated by algorithmic and algorithmic-driven fiscal operations, BI must proactively address these challenges and reinforce its commitment to its foundational mandate.

2.6. Social implications dimension of algorithmic systems

As organizations increasingly adopt algorithmic systems in financial services, such as fraud analysis, insurance claims, and payment, they must be aware of potential pitfalls, especially those arising from biases. Organizations should remain vigilant when implementing automated decision-making, taking preventative measures to minimize the risks of bias, and implementing corrective and compensatory actions when issues arise. The advent of algorithmic systems in finance presents a dual challenge: while they facilitate data collection from customers, they also threaten privacy (Bartneck et al., 2021; Chou, 2020; Perera et al., 2015). In the BI context, deploying algorithmic systems for fraud detection, risk assessment, and payment processing offers unprecedented efficiency and accuracy. This technological advancement, however, comes with societal costs. Automated decision-making processes risk perpetuating or exacerbating existing socioeconomic disparities if not properly designed and monitored. For example, algorithmic bias in credit scoring models can disproportionately affect marginalized communities, potentially leading to systemic financial exclusion (Jammalamadaka & Itapu, 2022).

Unlike traditional methods of data analysis and research, modern big-data research relies on a variety of public and private data sources that are both comprehensive and diverse (Perera et al., 2015). Once the data is analyzed, patterns are identified, and future trends are predicted. Privacy policies must explicitly state the permission to use such information, ensuring individuals understand the purposes and mechanisms underlying their use of personal data. Mahanti (2021) suggests that addressing this ethical challenge requires robust data governance measures.

The social ramifications extend beyond immediate financial concerns. As algorithmic systems become more prevalent in monetary policy decisions, there is a risk of creating a 'black box' economy, where the rationale behind financial regulations and interventions becomes increasingly opaque to the general public. This opacity could widen the knowledge gap between financial institutions and average citizens, exacerbating issues related to financial literacy and economic empowerment. Table 1 below summarizes the potential risk factors of introducing algorithmic systems into financial services that may impact financial stability and payment systems.

Table 1
Risk factors regarding algorithmic systems implementation in financial systems stability.

Risk Factor	Description	Source
Cyberattacks	The increasing complexity and interconnectedness of algorithmic systems make them more vulnerable to attack, potentially disrupting financial markets and payment systems.	(Maurer & Nelson, 2021; Schwartz, 2015; Taddeo et al., 2019; Violino, 2022)
Market Manipulation	The speed and complexity of algorithmic-enabled trading can lead to potential price manipulation, creating instability and reducing market fairness.	(Arnoldi, 2016; Faghan et al., 2020; Fletcher, 2021)
Systemic Risk	A vulnerability or failure in networked algorithmic systems could propagate and lead to potential system failure and monetary instability.	(Daníelsson et al., 2022; Jalan & Matkovskyy, 2023; Svetlova, 2022)
Financial Privacy	Algorithmic systems' data processing capabilities may raise significant privacy concerns and potential misuse of personal financial data.	(Bartneck et al., 2021; Tucker et al., 2019; Zhu et al., 2021)
AI Model Risk	Algorithmic models may fail to predict or respond appropriately to new situations, leading to incorrect decisions and potential financial losses.	(Akter et al., 2021; Belenguer, 2022; Bussmann et al., 2020; Hsu, 2022)
Bias in AI	Machine learning models may inadvertently acquire and persist biases, resulting in unfair or discriminatory practices within the financial sector.	(Akter et al., 2021; Belenguer, 2022; Hsu, 2022; Lin et al., 2021)
Regulatory Risk	The rapid development of algorithmic systems may outpace relevant regulations, leading to uncertainty and potential liabilities.	(Hsu, 2022; Theodorou & Dignum, 2020)
Dependency and Lack of Transparency	Overreliance on algorithmic systems could lead to a lack of understanding or transparency in decision-making processes, making it difficult to troubleshoot.	(Bussmann et al., 2020; Hind, 2019)

3. Data and methodology

3.1. Data

We conducted qualitative research through multiple interviews to explore the GELSI dimensions of algorithmic systems in financial services and to address our research question. To ensure a comprehensive understanding, we carefully selected a diverse sample of 18 participants from both academic and professional sectors. Academic participants were chosen for their interdisciplinary expertise in law, IT, and data science. These experts provided deep theoretical insights and a nuanced understanding of the broader implications of algorithmic systems within the GELSI framework. Their varied disciplinary knowledge ensures a well-rounded academic perspective. Professionally, we curated a mix of IT specialists, legal practitioners, bankers, and finance professionals. These individuals were selected for their hands-on experience with algorithmic systems in financial services, offering practical insights into the challenges and opportunities in this field. The diversity within this group allowed us to capture a wide range of perspectives from those directly involved in the application and regulation of these systems.

We prioritized participants with significant field experience to ensure the credibility and depth of the insights gathered. The majority of interviewees (59%) had over a decade of professional experience, while the remaining participants had at least five years of expertise. This depth of experience was crucial for obtaining nuanced and informed perspectives on the GELSI dimensions of algorithmic governance. The

Table 2
Demographics of interviewees.

Interviewee	Expertise	Category	Years of Experience
1	Academic and IT Consultant	Academic	>10 years
2	Law Practitioner	Practitioner	>10 years
3	IT Expert	Practitioner	5–10 years
4	Academic, Law Practitioner	Academic	5–10 years
5	Academic, Cyberlaw Practitioner	Academic	>10 years
6	Academic, Law Practitioner	Academic	>10 years
7	Banker	Practitioner	5–10 years
8	Finance Professional	Practitioner	5–10 years
9	Data Scientist at a Finance Company	Practitioner	5–10 years
10	Academic, Law Practitioner	Academic	>10 years
11	Finance Professional	Practitioner	5–10 years
12	Academic, Law Practitioner	Academic	>10 years
13	Banker	Practitioner	5–10 years
14	Academic, Cyberlaw Practitioner	Academic	5–10 years
15	Academic, Data Scientist	Academic	>10 years
16	Banker	Practitioner	>10 years
17	Law Practitioner	Practitioner	5–10 years
18	Finance Professional	Practitioner	5–10 years

selection strategy aimed to provide a holistic view of the topic by balancing theoretical knowledge with practical experience. Demographic characteristics of the participants are presented in Table 2.

The interviews explored various aspects of algorithmic systems in finance, including data regulation, privacy concerns, biases, and strategies for mitigating these risks. Participants assessed the role of financial institutions, the relevance of Indonesian legal frameworks, and the potential negative impacts, such as economic losses and emerging risks. The discussion also focused on strengthening financial authorities and leveraging technology to enhance payment systems and ensure monetary stability. Additionally, the participants rated the importance of critical dimensions for mitigating algorithmic risks, highlighting key priorities for effectively managing these challenges.

3.2. Methodology

Qualitative methods, such as interviews, provide deep insights into participants' reasoning, which quantitative approaches often overlook (Tracy, 2020). This study utilizes Interpretive Phenomenological Analysis (IPA) to explore how professionals navigate governance, ethics, legal, and social concerns within Indonesia's evolving regulatory landscape (Smith et al., 2009). IPA allows for a nuanced understanding of the meaning participants attach to their experiences. Interviews were transcribed verbatim and analyzed through thematic analysis to identify patterns aligned with the GELSI framework. To complement this qualitative depth, we also employed the AHP, a multi-criteria decision-making tool, to quantify the relative importance of the GELSI dimensions (Brunelli, 2015; Silva et al., 2023; Tavana et al., 2023). AHP involves defining criteria from the literature, conducting expert interviews, and constructing pairwise comparison matrices to assess the significance of each dimension. Consistency ratios were calculated using the eigenvalue method to ensure reliability (acceptable threshold: <0.10). The resulting priority weights provide a structured evaluation to guide informed conclusions (see Table A1, Appendix A).

IPA and AHP offer distinct advantages over quantitative methods, such as factor analysis and latent factor models (Ahelegbey et al., 2019; Arslan et al., 2022; Chang & Hsieh, 2024). While factor analysis identifies latent constructs, and latent factor models extract hidden factors via singular value decomposition, these techniques are best suited for numerical data. Given that our study relies on expert interviews, IPA, and AHP are more closely aligned with our research objectives. By combining IPA's qualitative depth with AHP's structured prioritization, this dual approach creates a comprehensive framework for analyzing algorithmic risk mitigation within Indonesia's emerging fintech regulatory environment. IPA allows us to uncover deep insights from experts, while AHP converts these insights into actionable priorities. This integrated methodology enhances decision-making in a field where subjective judgment plays a critical role. This integrated methodology strengthens decision-making in a domain where subjective judgment is crucial (see Table A2, Appendix A, for details).

4. Findings and analysis

This section presents the findings from our interviews, confirming the proposed GELSI framework based on the perspectives shared by our participants. The findings are organized into two sections: Governance and Ethical Dimensions; and Legal and Social Implications Dimensions. Each section outlines the key insights and observations drawn from the study, offering a detailed understanding of how algorithm systems are navigated within Indonesia's financial landscape.

4.1. Governance and ethical dimensions

Effective data governance is essential for operational success in the fast-paced financial and fintech industries. INV17 conveyed the crucial role of data governance, which extends beyond procedural requirements. This includes strict adherence to data protection measures and personal data regulations, safeguarding individual data, and reinforcing the trust that supports these industries.

Beyond basic data protection, INV15 offered a more comprehensive view, suggesting that data governance should encompass user education. Transparency is essential, shedding light on internal processes that handle and utilize data. Human involvement is equally crucial in safeguarding against the potential pitfalls of purely automated systems. Organizations can ensure privacy, mitigate biases, and uphold stringent accountability standards by maintaining a human touch in algorithmic processes.

The principles of confidentiality, integrity, and availability—often called the CIA triad—form the bedrock of effective data governance, particularly in sectors that rely heavily on data-driven decisions. These principles are not just guidelines but represent a commitment to protecting, preserving, and ensuring access to data in ways that uphold trust and maintain operational effectiveness. INV9 emphasized safeguarding confidential information, ensuring data integrity, and maintaining system accessibility—all of which are crucial for preventing breaches and ensuring the continuity of essential services.

The multifaceted nature of data governance presents unique challenges, particularly when considering the various stages of the data lifecycle. From initial data collection to eventual destruction, each stage demands a tailored approach to management and protection. INV11 highlighted the critical importance of consistent oversight and protection throughout this life cycle, while INV8 noted the need to view data as an ongoing flow rather than separate units.

Maintaining cutting-edge technical infrastructure and robust security measures is essential in today's fast-paced technological environment. INV11 and INV18 outlined proactive steps to strengthen digital landscapes, including implementing updated technical systems and integrating secondary backups to ensure continuity and resilience. Strengthening security infrastructure is equally important, as it adds layers of protection against unauthorized access and ensures that sensitive actions undergo thorough scrutiny before execution.

The rise of algorithmic systems offers unprecedented advancements but also presents significant ethical challenges. INV12 highlighted the need for a robust code of ethics specifically designed for algorithmic systems. Such a code would serve as both a guideline and a compass, directing the development and application of these systems to maximize benefits while mitigating risks. However, as INV4 pointed out, the mere existence of ethical guidelines is insufficient; their true impact lies in practical implementation. Recognizing and respecting the ethical boundaries of algorithmic systems ensures that technological progress remains grounded in moral responsibility. As these systems continue to shape the future, ethical guidelines play a crucial role in ensuring their responsible and humane evolution.

As algorithmic systems become increasingly integrated into modern society, transparency, and explainability in their development processes have become more critical than ever. INV3 emphasized the necessity of transparency, particularly for companies with extensive influence and reach. Stakeholders, consumers, and regulators demand visibility into the algorithms that drive these systems, not only to build trust but also to ensure that these algorithms are free from biases, uphold fairness, and align with societal values.

Achieving transparency in algorithmic system development is, however, challenging. INV6 highlighted the tension between the need for transparency and the protection of intellectual property. Companies must strike a balance by disclosing enough information to ensure accountability while safeguarding proprietary knowledge. Both INV3 and INV6 agreed that while transparency and explainability are essential, they remain complex issues in the rise of algorithmic systems. Striking a balance between disclosure and protecting proprietary knowledge is crucial in this era of algorithmic-driven innovation (see Table A3 in Appendix A, summarizing our findings and relevant interview excerpts related to governance and ethical dimensions).

4.2. Legal and Social Implications Dimensions

In the fast-moving world of digital innovation, government regulations, and law enforcement play a crucial role in ensuring the ethical deployment of new technologies, particularly algorithmic systems. Insights from the interviews underscored the urgent need for robust and unified governance. INV1 advocated for a proactive governmental stance, emphasizing the necessity of establishing minimum standards for algorithmic governance. These standards would serve as a baseline for ethical deployment and help prevent misuse before it occurs. Similarly, INV16 highlighted the critical role of oversight by established entities, such as BI and IT regulators, particularly in sectors that handle sensitive information. The enactment of the Personal Data Protection Law (UU PDP) in 2022 further reinforces the need for a structured approach to enforcing data protection regulations effectively.

INV17 added a crucial dimension to this discourse: awareness. Data protection extends beyond regulations to foster a culture of vigilance. Both private companies and government entities must recognize the significance of personal data. Moreover, law enforcement agencies require the necessary tools and knowledge to effectively address and resolve data protection issues. As the financial sector navigates an era of rapid technological progress and complex data governance challenges, the importance of a unified, cooperative approach among stakeholders has become increasingly evident. INV13 highlighted these complexities and emphasized the need for collaboration. The stakes are high, given the vast amounts of data generated, stored, and processed, particularly in the financial sector. Ensuring the security, privacy, and integrity of these data demands robust systems and collective efforts.

Collaboration among stakeholders enables entities in the financial industry to share best practices, pool resources, and address potential vulnerabilities. This synergy not only strengthens the resilience of the entire ecosystem but also safeguards the interests of both businesses and consumers. Amid the digital revolution, a new challenge emerges: ensuring that individuals understand the intricacies of the digital landscape. Digital literacy empowers users to navigate the digital world confidently and securely. Insights from INV15 highlighted this pressing concern, particularly within the financial sector. INV15 depicted the current scenario, in which users' lack of data literacy poses significant risks. This knowledge gap can lead to uninformed decisions, increased susceptibility to fraud, and misplaced trust in unreliable platforms. The financial sector must simplify data governance and make it more accessible to users. INV15 emphasized the importance of user-friendly mechanisms and transparency in fostering trust and informed decision-making. Digital literacy is not just about safe navigation, it is also about unlocking the full potential of the digital era.

However, while data protection laws are essential, they raise concerns about fairness and equity, particularly for economically disadvantaged individuals. INV14 expressed concern that the UU PDP, though a positive step toward safeguarding people's interests, may favor businesses over individuals. Rooted in the principles of protection and equality, the act emphasizes the prevention of discriminatory data processing, which could result in economic losses for data subjects. To bridge the gap between legislative intent and public perception, the UU PDP outlines a multifaceted approach to raising awareness. This includes training programs, public campaigns, and fostering citizen participation in data protection oversight.

The Act also enshrines the right of data subjects to receive comprehensive information about the processing of their personal data, including its purpose and preservation methods. To empower citizens, particularly those who are economically disadvantaged, the law must be complemented by robust awareness campaigns, educational initiatives, and accessible support systems. By implementing a systemic literacy framework and establishing mechanisms to measure public understanding of data processing, the UU PDP can evolve from mere legislation into a powerful tool for individual empowerment in the digital age (see Table A4 in Appendix A summarizing our findings and relevant interview excerpts related to the legal and social implications).

4.3. Additional dimensions emerge from respondents

Mitigating algorithmic risk in finance requires attention to several critical factors. Established national and international frameworks, such as those from the International Organization for Standardization (ISO), provide a structured blueprint for managing and mitigating cybersecurity risks. As INV10 suggested, these frameworks encapsulate best practices for addressing specific sectoral needs. System design and planning are crucial. A robust system architecture, supported by comprehensive Incident Response, Disaster Recovery, and Business Continuity Planning (IRP, DRP, and BCP), ensures resilience against cyberattacks and guarantees rapid recovery from disruptions. INV18 emphasized that these systems not only protect financial infrastructure but also preserve trust and operational stability.

The algorithms that power these systems deserve scrutiny. INV15 reflected on the importance of transparency explanations of confidence levels and algorithmic decisions. Such transparency bolsters trust, facilitates comprehension, and empowers stakeholders to identify potential bias and errors. Resources are the backbone of any effective cybersecurity initiative. A robust support network that includes government entities, cybersecurity experts, implementers, and technologically adept legal professionals fortifies the framework. INV15 reinforced the significance of enforcement mechanisms, which serve as potent deterrents by emphasizing the consequences of non-compliance and fostering a culture of accountability. In the rapidly evolving digital landscape, leveraging cutting-edge solutions such as Regulatory Technology (Regtech) and Supervisory Technology (Suptech) has become vital. These tools enhance regulatory compliance and supervisory capabilities, ensuring real-time monitoring and control of emerging cybersecurity risks. Table 3 summarizes and details the additional dimensions that emerged from the interviews.

4.4. Relevancy of GELSI framework through MSA framework

Following the findings above, we also investigated the relevance of

Table 3
Additional dimensions for algorithmic systems' risk mitigation.

Additional Dimensions	Explanation
• Implementation of Framework – National or International Standard (e.g., ISO).	Adopt established cybersecurity frameworks like ISO tailored to the financial sector's needs.
• System Design and Planning, including IRP, DRP, and BCP.	Implement robust system architecture, BCP, and DRP to withstand cyberattacks and recover from disruptions.
• Explanation of capabilities and confidence level of algorithms - Bayesian Learning with Deep Learning.	Enhance transparency by explaining the capabilities and confidence levels of algorithmic systems, like Bayesian Learning with Deep Learning.
• Algorithmic Performance Audit and Evaluation.	Regularly audit and evaluate algorithmic systems to ensure accuracy, reliability, and standard adherence.
• Guidelines on quantifying damages/risks due to personal data violations.	Set guidelines to assess damages and risks from personal data violations for appropriate responses.
• Resources (including government, implementers, economic actors, and legal talents who understand technology).	Ensure skilled resources from the government, cybersecurity experts, implementers, and tech-savvy legal professionals.
• Enforcement Consequences.	Implement strict mechanisms for non-compliance, serving as a deterrent for organizations.
• Regtech and Suptech.	Use Regtech and Suptech solutions to enhance regulatory compliance and supervisory capabilities.

MSA in formulating a framework for algorithmic system governance in finance. Our analysis revealed how the three streams (i.e., problem, policy, and politics) converge to create a comprehensive picture of the current landscape and potential forward paths.

The problem stream was evident in the identified challenges, such as issues in data governance (INV17, INV15), the need for robust security protocols (INV8, INV9, INV11), and ethical concerns regarding algorithmic systems (INV11, INV4). As outlined by various interviewees, these problems represent critical issues that policymakers must address. These findings highlight the necessity of proactive government regulation (INV1), the importance of raising data protection awareness (INV17), and the pervasive lack of digital literacy among users (INV15). These issues present a compelling case for policy action. Additionally, the problem stream reveals the need for robust system design, algorithmic transparency, and methods to quantify the risks associated with data violations, which are vital concerns in the financial sector.

A policy stream emerged in the proposed solutions and guidelines, such as developing ethical frameworks for algorithmic systems (INV11), implementing updated technical systems, and establishing transparency and explainability measures (INV6). These proposals reflect potential policy responses to the identified problems. The policy stream was also evident in calls for specific actions, such as establishing minimal standards for algorithmic systems governance (INV1), implementing structured approaches to enforce data protection regulations (INV16), and developing educational programs to enhance digital literacy (INV15). Moreover, the policy stream highlights proposed solutions, such as adopting national and international standards, developing IRP, DRP, and BCP, and utilizing Regtech and Suptech for improved compliance and supervision.

The political stream was implicit in discussions about regulatory compliance, the role of associations in crafting codes of conduct, and the need for independent oversight organizations (INV4). These elements suggest the political and organizational contexts within which policies must be developed and implemented. The political stream also emphasized collaboration among financial bodies (INV13) and the need for a balanced approach that considers business interests and individual rights (INV14). The political context shapes the feasibility of potential policy solutions. Furthermore, the political stream reflected discussions about enforcement consequences, the necessity of skilled resources across government and private sectors, and the challenges of collaborating with financial institutions. These elements demonstrate the political and organizational environments in which policies must take shape.

MSA's concept of policy windows is particularly relevant in the fast-evolving financial technology sector, where rapid technological advancements may create opportunities for policy changes. The role of policy entrepreneurs is crucial in solving coupling problems, as suggested by the interviewees' emphasis on proactive measures and collaborative approaches. MSA's recognition of policy windows allows policymakers to capitalize on moments when public attention is focused on issues such as data breaches or algorithmic biases to advocate for comprehensive regulatory frameworks. Moreover, the concept aligns with the roles of various stakeholders mentioned in the findings, such as regulators, financial institutions, and advocacy groups, who can couple problems with solutions and navigate the political landscape. MSA's recognition of policy windows aligns seamlessly with the dynamic nature of financial technology, where emerging technologies and regulatory challenges present unique opportunities for policy evolution.

4.5. Prioritizing dimensions in the GELSI framework: insights from AHP analysis

Based on the interview responses, we applied the AHP to weigh the dimensions in the proposed GELSI framework, helping prioritize components essential for robust data governance. The AHP process used a pairwise comparison matrix, where values quantified the relative importance of dimensions, leading to systematic ranking. 'Ethical Guidelines for Algorithmic Systems' and 'Data Classification, Management, and Storage' emerged as top priorities, emphasizing ethical and organizational accountability in data handling. Other high-ranking dimensions included 'Proper and Robust Data Governance', 'Updated Technical Systems and Protocols', and 'Solid and Robust Government Policies'. While deemed essential, lower-ranked dimensions, such as 'Legal Support for Economically Disadvantaged Individuals' and 'Collaborative Accord between Organizations', carried less weight in immediate strategic impacts. The 8% Consistency Index suggested strong coherence, reinforcing the reliability of the rankings. This analysis indicates the critical importance of ethical and structured data practices in effectively managing algorithmic systems, providing a foundation for future policy and strategy improvements in digital governance (see Appendix B for a detailed explanation of the AHP process).

5. Discussion

As algorithmic systems have gained prominence in financial services, their challenges have become increasingly pressing in countries such as Indonesia, where the central bank is paramount in maintaining monetary stability and overseeing payment transactions. The GELSI framework offers a holistic approach to mitigating the complexities of integrating AI and financial systems (see, Tables 4 and 5).

First, under the 'Governance' dimension, there is a pressing need to address cyberattacks and AI model risks (Taddeo et al., 2019). As Indonesia moves toward a digital economy, ensuring the robustness of its financial algorithms becomes crucial. The solution lies in establishing proper data governance, updating technical systems, reinforcing security protocols, and emphasizing confidentiality, integrity, and availability. This ensures that as Indonesia's financial system becomes increasingly digitized, it remains resilient against external threats.

The 'Ethical' aspect of the framework explores concerns about financial privacy, biases in AI, and the potential pitfalls of over-relying on algorithms without transparent oversight (Floridi, 2021; Floridi et al., 2021; Palladino, 2022). Indonesia can foster trust in its digital financial ecosystem and ensure equitable outcomes by implementing AI ethical guidelines and emphasizing transparency and explainability in the AI development processes.

From a legal perspective, introducing regulatory measures, such as harmonizing regulations and fostering collaboration among financial institutions, can address potential regulatory risks. As Indonesia's central bank oversees monetary stability, establishing clear legal parameters ensures that AI-driven financial innovation aligns with its economic goals.

Lastly, the 'Social Implications' dimension recognizes the broader societal implications of algorithmic systems in finance. By promoting digital literacy campaigns and providing legal aid for marginalized groups, Indonesia can ensure that the benefits of AI-driven financial services are accessible and beneficial to all. Overall, the GELSI framework serves as a strategic roadmap for BI. By addressing the challenges of integrating algorithmic systems into financial services through this framework, banks can pave the way for Indonesia's secure, ethical, and inclusive financial future.

The additional emerging dimensions in the GELSI framework offer new avenues for risk mitigation and efficiency in financial services. Framework Implementation stresses adopting ISO standards and sector-specific frameworks to ensure consistent compliance and adaptation. System Design focuses on continuity planning, emphasizing robust architecture and disaster recovery to maintain operations. Algorithm Evaluation introduces regular performance audits and bias testing to safeguard fairness and effectiveness. Resource Management prioritizes skilled personnel, supported by training and resource allocation. Lastly, Regtech/Suptech enhances oversight through automated compliance and real-time risk assessment, reinforcing regulatory capabilities, and offering resilient, responsive governance solutions.

Table 4
Proposed GELSI framework.

Framework Dimension	Component	Description	Risk Mitigation Approach
Governance	Data Governance	Manages data confidentiality, integrity, availability	• Data protection measures • Enforce personal data regulations • Lifecycle oversight
	Data Classification	Systematic handling and securing of data	• Sensitivity-based classification • Security per classification • Quality assessments
	Technical Systems	Updated systems and security protocols	• System updates • Backup implementations • Security infrastructure
Ethical	Ethical Guidelines	Frameworks for algorithmic systems	• AI ethics code • Ethical audits • Innovation-moral balance
	Transparency	Clear algorithmic development processes	• Visibility in operations • Disclosure-IP protection • Stakeholder communications
	Accountability	Responsibility for algorithmic decisions	• Accountability frameworks • Human oversight • Performance monitoring
Legal	Regulatory Compliance	Adherence to laws and regulations	• PDP Law implementation • Compliance audits • Updated frameworks
	Enforcement	Ensures compliance mechanisms	• Enforcement procedures • Non-compliance penalties • Regulatory reviews
	Cross-border Considerations	International regulatory alignment	• Global standards compliance • International cooperation • Harmonized regulations
Social Implications	Digital Literacy	User education and awareness	• Education programs • Clear risk communication • User-friendly interfaces
	Economic Impact	Protection of vulnerable users	• Support disadvantaged groups • Fair access • Economic impact assessments
	Public Trust	Confidence in systems	• Transparent communication • Stakeholder engagement • Awareness campaigns

Table 5
Additional dimensions for GELSI framework.

Dimension	Description	Risk Mitigation Approach
Framework Implementation	National/International Standards	• ISO standards • Industry frameworks • Framework updates
System Design	Business Continuity Planning	• System architecture • Disaster recovery • Response procedures
Algorithm Evaluation	Performance monitoring and assessment	• Algorithmic audits • Performance metrics • Bias testing
Resource Management	Skilled personnel and infrastructure	• Expert recruitment • Training programs • Resource allocation
Regtech/Suptech	Regulatory technology solutions	• Automated compliance • Real-time risk assessment • Enhanced supervision

6. Contributions

6.1. Theoretical contributions

Our study integrates MSA to provide a comprehensive framework for developing and implementing responsible algorithmic financial system policies (Jones et al., 2016; Kingdon, 2003). This approach offers fresh insights into algorithmic system governance and addresses the complex challenges of modern technological advancements in the financial sector. The MSA's problem stream aligns seamlessly with our qualitative findings, offering a nuanced lens for identifying and framing critical issues in algorithmic finance. Complementing this, our AHP analysis elevates ethical guidelines and data governance as paramount concerns, underscoring policymakers' need to prioritize these elements on the legislative agenda. This dual approach to problem framing highlights pivotal issues, ensuring that they receive commensurate attention in policy deliberations.

In the policy stream, our qualitative-derived insights yield solutions that honor human dignity, autonomy, and universal moral principles. This stream, informed by AHP prioritization, guides the creation of robust governance frameworks, data protection standards, and risk management strategies tailored to the unique challenges of algorithmic systems in finance. Our findings emphasize the critical role of updated technical protocols and solid government policies in shaping effective regulatory responses. The political stream has emerged as a crucial conduit for molding national sentiment and the discourse surrounding algorithmic systems in finance. This stream fosters political will and public trust by accentuating the imperatives of ethical AI utilization and data protection, as reflected by our qualitative analysis. Our AHP analysis further reinforces the significance of transparency, explainability, and digital literacy campaigns in cultivating a favorable environment for policy adoption and implementation.

Our study, grounded in rich qualitative data and prioritization insights from AHP, resonates with MSA's emphasis on policy windows and coupling. This methodological synergy offers a dynamic framework for policymakers to link problems with solutions as opportunities arise, enabling agile and targeted responses to emerging challenges in algorithmic finance. The MSA's applicability to comparative policy analysis, enhanced by our multi-method approach, bolsters our effort to develop ethical guidelines that transcend cultural and national boundaries—a

crucial consideration in our interconnected global financial ecosystem.

We acknowledge the inherent complexities and ambiguities of algorithmic system policymaking, as revealed by our IPA and AHP analyses. The MSA's recognition of these challenges and our empirical findings provide a nuanced framework for navigating ethical intricacies within practical constraints. This approach facilitates the development of adaptive regulatory frameworks capable of evolving with technological advancements and shifting risk landscapes in AI and finance. Table 6 presents our theoretical contributions, guided by MSA, for algorithmic governance.

Table 7 illustrates two distinct policy scenarios using MSA that involve cryptocurrency regulation and open banking implementation, highlighting the dynamic interplay between technological advancement, regulatory response, and political influence. Both scenarios demonstrate the necessity of aligning problem identification, policy solutions, and political will, illustrating how external crises and successful precedents can create policy windows that enable significant regulatory advancements.

6.1.1. Scenario 1: Cryptocurrency regulation

In the problem stream, the rapid adoption of cryptocurrencies in Indonesia presents complex challenges, where algorithmic systems and AI-driven mechanisms play a pivotal role. The integration of AI and blockchain technology in cryptocurrency transactions introduces both opportunities and risks, as AI enhances algorithmic trading efficiency while blockchain ensures decentralization and security. However, AI-powered trading mechanisms and smart contracts also raise significant concerns regarding monetary stability (Giudici et al., 2022; Omohundro, 2014; Vo & Yost-Bremm, 2020). These automated systems can execute high-frequency trades at unprecedented speeds, potentially amplifying market volatility and systemic risks (Li & Huang, 2020; Zhang & Ding, 2021). Traditional financial systems struggle to cope with AI-driven algorithmic trading bots that can exploit market inefficiencies, while decentralized digital assets operate beyond conventional regulatory frameworks. The challenge lies in ensuring that AI-augmented algorithmic systems do not undermine financial stability while leveraging blockchain's immutable and transparent nature to enhance security.

Table 6
Theoretical insights and contributions of MSA to algorithmic governance.

MSA Component	Theoretical Findings	Contribution to Algorithmic Systems Governance in Finance
Problem Stream	Identifies and frames key issues in algorithmic systems, such as data governance, algorithmic biases, and financial stability threats, to prioritize them on the policy agenda.	Ensures that critical issues are recognized and elevated in policy discussions, making them central to policymaking efforts.
Policy Stream	Informs the development of ethical, practical policy solutions, including governance frameworks, data protection standards, and risk management strategies for algorithmic systems in finance.	Guides the creation of robust, ethically grounded policies that address the unique challenges of algorithmic systems in the financial sector.
Political Stream	Shapes the national mood and political discourse, building political will and public trust to create a favorable policy adoption and implementation environment.	Facilitates broad support and effective enactment of policies, ensuring that they are politically viable and publicly endorsed.
Policy Windows & Coupling	Highlights the importance of linking problems with solutions during opportune moments, enabling swift and targeted responses to emerging challenges in algorithmic finance.	Allows policymakers to capitalize on heightened public and political focus, ensuring timely and relevant policy responses to algorithmic issues.

In response, the policy stream can propose several algorithmically driven regulatory measures that acknowledge the dual role of AI and blockchains in securing cryptocurrency markets. AI-driven algorithms must balance transaction efficiency with security by incorporating machine learning for real-time risk assessment while leveraging blockchain's transparency to ensure trust. Regulatory frameworks for crypto assets require advanced AI-driven algorithmic surveillance systems to track cross-border transactions and identify potential money laundering activities. Furthermore, stress testing of AI-powered trading systems should be mandated to assess their impact on market stability, ensuring that blockchain's security mechanisms are not compromised by unregulated AI-driven speculation.

The political stream reflects growing public awareness of the impact of AI-enhanced algorithmic trading on market dynamics. Traditional financial institutions have expressed concerns about the sophisticated AI algorithms employed in decentralized finance, which could potentially outperform conventional trading systems while operating outside traditional oversight structures. International regulatory developments have increasingly focused on AI and blockchain transparency and accountability, particularly in automated trading systems and smart contract execution. The intersection of AI and blockchain governance is now a key consideration in shaping policy responses to algorithmic trading.

A policy window occurs when a major cryptocurrency exchange collapses, revealing vulnerabilities in AI-driven algorithmic trading systems and blockchain-based financial infrastructure, leading to significant market disruption. This crisis will allow BI to implement comprehensive digital asset regulations focusing on algorithmic governance, ensuring that AI-driven trading mechanisms are subjected to rigorous oversight while leveraging blockchain's auditability. The public, now acutely aware of the risks posed by unregulated AI-powered trading systems, supports stronger oversight measures. This enables policymakers to introduce robust regulatory frameworks that specifically address AI-enhanced algorithmic risks in cryptocurrency markets, including requirements for algorithmic auditing, transparency in AI-driven trading bot operations, and stress testing of automated trading systems to mitigate systemic risks while preserving the security benefits of blockchain technology.

6.1.2. Scenario 2: Open banking implementation

In the problem stream, the dominance of traditional banks highlights significant algorithmic challenges in the financial sector. Legacy banking systems often rely on outdated credit scoring and risk assessment algorithms, which limit financial inclusion and innovation (Suhadolnik et al., 2023). These conventional algorithmic models, built on historical data, can perpetuate existing biases and restrict access to financial services for underserved populations. Moreover, the lack of standardized algorithmic interfaces between institutions creates technical barriers, preventing efficient data sharing and limiting the development of innovative financial solutions (Sargeant, 2023).

The policy stream focuses on developing sophisticated algorithmic frameworks that enable open banking. This includes standardized API protocols powered by machine-learning algorithms that can securely manage data exchange between institutions while maintaining data integrity (Frei et al., 2023). Advanced algorithmic systems for real-time fraud detection and authentication should be proposed to ensure secure data sharing across platforms. New algorithmic models for privacy-preserving computation can also be developed to enable data analysis without compromising sensitive information, thus addressing both innovation and security concerns.

The political stream reveals tensions in algorithmic governance. Fintech companies advocate for access to banking data to develop more sophisticated algorithmic models for credit scoring and personalized financial services (Sargeant, 2023). Consumer groups push for transparency in algorithmic decision-making, particularly in automated lending and risk assessment systems. Traditional banks, however, may

Table 7
MSA application to relevant scenarios in Indonesia.

Scenario	Problem Stream	Policy Stream	Political Stream	Policy Window
Scenario 1: Cryptocurrency Regulation	• Increasing adoption of cryptocurrencies • Potential threats to monetary stability • Consumer protection concerns	• Creation of regulatory frameworks for crypto assets • Implementation of licensing requirements for crypto exchanges	• Public demand for digital payment alternatives • Pressure from traditional financial institutions • International regulatory developments	A major cryptocurrency exchange collapse creates an opportunity for BI to implement comprehensive digital asset regulations while maintaining public support.
Scenario 2: Open Banking Implementation	• Limited competition in banking services • Consumer data accessibility issues • Technical barriers to financial innovation	• Development of application programming interface (API) standards • Data sharing protocols • Security and privacy frameworks	• Fintech industry advocacy • Consumer rights groups support • Traditional banks' resistance	Successful implementation of open banking in other regions creates momentum for adoption, while increasing cyber threats highlight the need for standardized security protocols.

resist sharing proprietary algorithms and data, viewing them as competitive advantages. A policy window emerges with successful open banking implementations in other regions, demonstrating the effectiveness of well-governed algorithmic systems. Simultaneously, rising cyber threats highlight the need for advanced algorithmic security protocols. This convergence creates momentum for implementing standardized algorithmic frameworks to facilitate secure data sharing while protecting against cyber risk. This window provides an opportunity to establish comprehensive guidelines for algorithmic governance in open banking, ensuring that innovation in financial services is balanced with robust security measures and ethical considerations in algorithmic decision-making.

6.2. Practical contributions and recommendations

6.2.1. Practical contributions on responsible algorithmic systems framework

The rapid advancement of algorithmic systems in finance has necessitated robust frameworks to ensure responsible implementation and regulation. While frameworks such as SAFE and IBM's Fairness 360 toolkit[11] offer valuable quantitative metrics and technical solutions, our GELSI framework provides a broader qualitative perspective that can significantly enhance these approaches in contributing to algorithmic trust and regulation.

GELSI's comprehensive focus on four overarching dimensions—governance, ethics, legal considerations, and social implications—complements SAFE's finance-specific quantitative metrics. While SAFE offers precise measurements of sustainability, accuracy, fairness, and explainability in financial AI systems, GELSI provides the crucial context within which these metrics operate. For instance, GELSI's governance dimension can help financial institutions and regulators interpret SAFE metrics within a larger organizational and regulatory framework, ensuring that quantitative assessments translate into meaningful policy and operational decisions. Similarly, GELSI can enhance IBM's Fairness 360 toolkit by providing a holistic view of fairness beyond statistical measures. While Fairness 360 offers sophisticated algorithms to detect and mitigate bias, GELSI's ethical and social implications considerations help organizations understand the broader impact of fairness in AI systems. This synergy allows for a more nuanced approach to fairness that considers mathematical equity alongside societal and ethical ramifications.

Integrating GELSI with SAFE and Fairness 360 can create a robust framework for building and maintaining public confidence in AI systems. GELSI's emphasis on transparency and accountability in AI governance aligns well with SAFE's explainability metrics and Fairness 360's bias detection tools. This alignment can help regulators develop comprehensive and effective oversight mechanisms that address both technical and societal concerns. Moreover, GELSI's legal dimension provides valuable insights into regulatory compliance, complementing the quantitative assessments of SAFE and Fairness 360. This integration helps financial institutions navigate the complex regulatory landscape of AI implementation, ensuring that their systems meet technical standards while complying with legal and ethical norms.

By combining these frameworks, stakeholders in the financial AI ecosystem can develop a holistic approach to algorithmic trust and regulation. This approach balances quantitative rigor with qualitative insights, technical proficiency with ethical considerations, and specific financial metrics with broader societal impacts. Such a comprehensive framework can significantly enhance the responsible development, deployment, and regulation of AI in finance, fostering greater trust among users, regulators, and the public.

6.2.2. Recommendation on GELSI Framework Implementation

BI plays a pivotal role in mitigating algorithmic risk in the rapidly evolving financial technology landscape. Drawing on MSA, we propose a multifaceted framework for BI to navigate the complexities of algorithmic system governance in finance. As problem-stream initiators, BI must focus on identifying and framing algorithmic-system-related challenges. This involves addressing data governance issues, algorithmic biases, and emerging cybersecurity threats (Daim and Dabić, 2023). By clearly articulating these problems, BI sets the stage for targeted policy responses.

In their capacity as policy-stream facilitators, BI should spearhead the development of robust algorithmic system governance frameworks. This entails crafting data protection standards and risk management strategies tailored to the nuances of the financial sector. Such proactive policy formulation lays the groundwork for practical regulatory actions. As political stream navigators, BI should deftly shape public discourse around algorithmic systems in finance. By emphasizing ethical algorithmic systems and data protection, they can build the political will and public trust necessary for implementing meaningful reforms.

BI must also be prepared to swiftly couple problems with solutions when policy windows open, such as by implementing new algorithmic system regulations in response to high-profile incidents of algorithmic bias. BI is uniquely positioned to facilitate collaboration across sectors. By bringing together financial institutions, tech companies, and regulatory bodies, it can foster a comprehensive approach to addressing algorithmic system challenges. Finally, BI must design flexible regulatory frameworks capable of evolving alongside technological advancements and the ever-changing risk landscapes of algorithmic systems and finance. By embracing these interconnected roles, BI can effectively leverage MSA to address the multifaceted challenges of algorithmic

[11] https://aif360.res.ibm.com/.

systems in the financial sector.

In the digital era, BI plays a crucial role in maintaining financial security and stability as algorithmic systems reshape finance. A key responsibility is data governance, where BI sets rigorous standards for data collection, storage, and protection, ensuring a trustworthy financial framework. Acting as data custodians, BI safeguards the confidentiality, integrity, and availability of financial data, reinforces defenses against cyber threats, and enhances systemic resilience. By aligning with global standards, such as ISO, BI promotes risk mitigation and systemic stability (Sánchez & De Batista, 2023; Shinde & Kulkarni, 2021). Beyond governance, BI evaluates algorithmic frameworks, ensuring fairness and accuracy (Boer et al., 2023; Le Merrer et al., 2023). Establishing rigorous standards helps eliminate biases in financial algorithms. As a privacy advocate, BI enforces data protection regulations, fostering public trust in financial institutions.

The emergence of regtech and suptech enables BI to monitor the financial sector with greater precision, mitigating systemic and regulatory risks (Ruof, 2023). As bridge builders, BI fosters cooperation through the memoranda of understanding among financial entities, promoting a unified strategy to address algorithmic risks. As compliance enforcers, BI ensures adherence to regulations, sanctions for violations, and maintaining financial discipline. As algorithmic systems evolve, BI's traditional macro-level focus must expand to address micro-level risks and tackle the challenges faced by individual entities that could trigger systemic disruptions. Fig. 1 and Table 8 outline BI's critical role in mitigating algorithmic risks in finance.

To fulfil its role, the BI should establish a regulatory framework that ensures consistent standards across the financial sector. This could involve issuing derivative regulations from UU PDP to specific BI regulations, thus offering clear guidance on data protection. BI can also develop regulatory or supervisory technologies to aid financial institutions in self-assessment and compliance, making adherence accessible and practical. Beyond traditional regulations, BI may oversee the creation of platforms that support compliance with algorithmic systems and data-governance standards. These tools can help businesses consistently implement best practices, providing a straightforward interface for reporting, monitoring, and managing algorithmic systems. This tech-forward approach would enhance not only regulatory adherence but also operational efficiency.

BI should focus on macro-level standards when implementing these recommendations, promoting system-wide resilience to cyber threats and advancing technological oversight. BI's role in data governance involves setting global standards, ensuring system interoperability across borders, and fostering financial system stability against failures and attacks, particularly those related to algorithmic systems. On a micro level, OJK (Indonesia's Financial Services Authority) would ensure financial institutions adhere to BI standards. This includes supervising data quality, evaluating algorithmic systems, enforcing compliance with data privacy regulations, and educating consumers on data rights. OJK's oversight ensures financial institutions effectively operationalize these frameworks, maintaining ethical standards, fairness, and accuracy in algorithmic systems. Collaboration between BI and OJK is essential for avoiding redundancy. BI provides the infrastructure and policy framework, whereas OJK ensures practical implementation, creating a resilient and compliant financial ecosystem in the face of evolving risk. Table 9 summarizes the roles of BI and OJK in mitigating algorithmic system risks.

The GELSI framework for algorithmic systems in finance faces significant challenges due to the rapid evolution of financial technology, which often outpaces regulatory efforts. BI must continuously update governance frameworks while ensuring regulators have the technical expertise to oversee complex algorithmic systems effectively. Balancing innovation and risk mitigation is critical—excessive regulation may stifle technological advancement, while insufficient oversight can lead to biases and cybersecurity threats.

Cross-sector collaboration is another challenge, as financial institutions and technology firms have diverse interests. Ensuring consistent implementation while maintaining market fairness adds complexity. Additionally, data privacy concerns arise from extensive data sharing and analysis, requiring a delicate balance between oversight and individual privacy rights. The global nature of financial markets further complicates regulation—without international coordination, national-level efforts may be insufficient. These challenges highlight the need for adaptive, flexible, and collaborative regulatory approaches involving ongoing dialogue among regulators, industry leaders, and technology experts.

Though designed for Indonesia, the GELSI framework is adaptable across various regulatory landscapes. Its modular structure allows jurisdictions to adjust implementation while maintaining its core principles. Governance, algorithmic fairness, and accountability are globally relevant concerns, regardless of regulatory environments. Legal adaptability is also key—while GDPR and CCPA differ, the framework's emphasis on data protection and algorithmic accountability provides a flexible template for various legal systems. Countries like Singapore focus on technological innovation with oversight, while the EU prioritizes consumer protection. The GELSI framework accommodates these variations, making it a valuable tool for central banks worldwide.

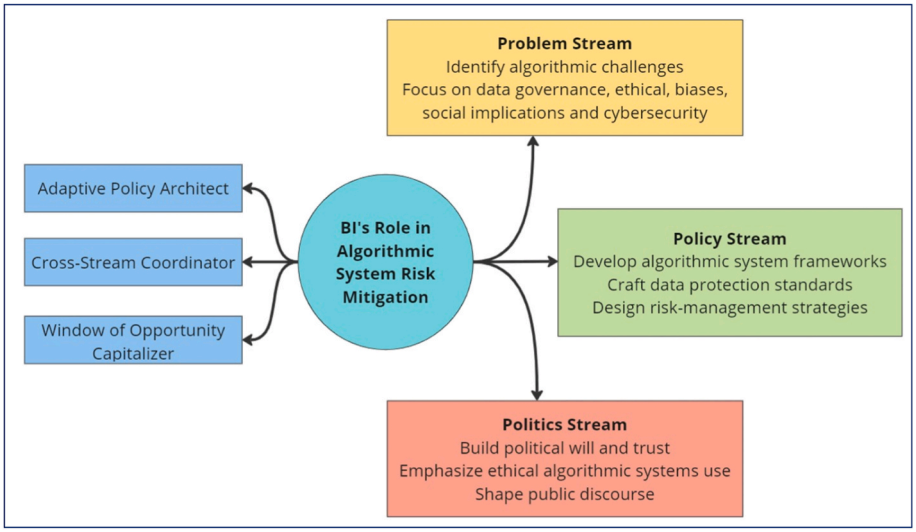

Fig. 1. BI's role in algorithmic system risk mitigation based on multiple stream approach.

Table 8
The central Bank's role in mitigating algorithmic in finance risk.

Role/Function	Description	How Bank Central Could Implement The Role?
Data Governance at Its Core	Set data standards for financial institutions. Ensure the uniformity and consistency of data across the financial sector. Promote data sharing and collaboration among financial institutions.	BI could set data standards for financial institutions, promoting uniformity and encouraging data sharing and collaboration, which benefits the financial sector's stability and innovation.
Guardians of Data	Enforce and oversee the implementation of high data quality standards within the financial sector. This includes mandating banks comply with UU PDP to responsibly handle personal data. By doing so, BI would not directly manage personal and private data but rather ensure that banks in Indonesia uphold the law and best practices for data protection.	This oversight reinforces the integrity and reliability of the financial data ecosystem, ensuring that the banks provide high-quality data that is accurate and managed in compliance with data protection laws. It also maintains consumer confidence in the financial system, knowing that their data is treated with the utmost care and complies with legal standards. BI's role would also extend to the continuous monitoring and auditing of banks to verify ongoing compliance and to take corrective actions when breaches or lapses in data quality or compliance occur.
Architects of System Robustness	Promote robust banking systems and standards. Design and implement algorithmic systems that are resilient to failures and attacks. Develop and implement risk management frameworks for algorithmic systems.	The institution's role in promoting resilient algorithmic systems can lead to a more robust financial sector capable of withstanding cyber threats, thus safeguarding the economy.
Evaluators of Algorithmic Systems	Implement ethical guidelines for algorithmic systems development and use while simultaneously verifying fairness and accuracy through testing and validation. Focus on identifying and eliminating any potential biases or discrimination in algorithmic systems.	Ensuring that algorithmic systems are fair and unbiased contributes to equitable financial practices, benefiting society by preventing discrimination.
Advocates of Data Privacy	Promote compliance with data protection regulations, foster trust by informing consumers about their data privacy rights, and support the development of robust data protection laws and regulations.	BI's enforcement of data protection can enhance consumer trust, ensuring individuals' privacy rights are respected.
Technology for Oversight	Use technology to monitor and oversee algorithmic systems in financial institutions. Develop and implement tools and techniques for detecting and preventing fraud and other financial crimes. Promote transparency and accountability in the use of algorithmic systems.	Utilizing technology for monitoring algorithmic systems in finance can help prevent fraud, benefiting individuals by protecting their assets.
Facilitators of Cooperation	Encourage collaboration among financial institutions to manage and monitor algorithmic systems effectively. Foster the exchange of effective strategies and insights. Create and enforce comprehensive industry standards and principles for algorithmic systems utilization.	Cooperation among financial institutions aids in comprehensive risk management, enhancing overall stability. This can be done through (1) hosting the industry forums for algorithmic systems risk management collaboration, (2) creating a shared database of algorithmic systems' risk case studies, (3) developing joint algorithmic systems risk management guidelines, (4) launching a platform for sharing algorithmic systems incident data. (5) offering algorithmic systems risk management training for financial institutions.
Enforcers of Compliance	Ensure adherence to standards for developing, deploying, and using algorithmic systems in financial institutions. Investigate and prosecute violations of data protection and other applicable laws and regulations. Promote a culture of compliance within the financial sector.	By ensuring adherence to algorithmic systems and data use standards, BI can foster a culture of compliance, which is crucial for the integrity of financial systems.

Table 9
The role of BI and OJK in implementing the initiative to mitigate algorithmic systems risk.

Role	BI	OJK
Data Governance	Set and ensure cross-border interoperability of data standards.	Operationalize and supervise adherence to these standards.
System Resilience	Lead development of resilient financial systems against cyber risks.	Ensure financial institutions comply with resilience standards.
Technological Oversight	Advance oversight technology for financial systems monitoring.	Monitor and enforce compliance in the use of algorithmic systems and related tech.
Regulatory Compliance	Advocate for strong data protection laws.	Educate consumers and enforce data privacy regulations.

7. Conclusion and limitations

The GELSI framework serves as a pragmatic strategy for developing and governing direct, actionable algorithmic systems. In practical applications, the dynamism of the digital age has been instrumental in enabling BI to ensure the stability and security of evolving financial systems. With broad mandates covering data governance and algorithm evaluation, BI focuses on building trust and confidence in an increasingly connected world. BI must harmonize global standards, champion data privacy, and leverage technological advancements such as regtech and suptech. However, its role is twofold: fostering collaborative efforts while ensuring strict compliance. As algorithmic systems reshape the financial landscape, BI stands at an evolutionary crossroads. Traditionally macro-focused, its scope has been expanded to address micro-level threats posed by individual entities that could trigger broader systemic challenges.

This study had several limitations. First, reliance on individual inputs and our interpretation of the data may have introduced bias into the analysis. Second, while the findings provide valuable localized insights within the Indonesian context, they may not fully capture the regulatory nuances of other regions or sectors. Differences in regulatory environments, industry practices, and financial challenges across countries may limit the generalizability of the GELSI framework. To address this limitation, future research should conduct comparative analyses of algorithmic risk mitigation in diverse geographical settings. Such studies could highlight the unique challenges and opportunities within various regulatory landscapes, contributing to a more comprehensive

understanding of global algorithmic governance in finance. Additionally, tracking the evolution of perspectives on algorithmic governance as technology and its associated challenges evolve would further enrich the discourse.

CRediT authorship contribution statement

Arif Perdana: Writing – review & editing, Writing – original draft, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Saru Arifin:** Writing – review & editing, Project administration, Investigation, Funding acquisition. **Novi Quadrianto:** Writing – review & editing, Investigation, Funding acquisition.

Acknowledgment

This research was funded by Research Grant Bank Indonesia through Grant No. 25/19/PKS/BINS/2023.

Appendix: A

Table A1
AHP Criteria Based on the GELSI Framework

Dimension	Criteria	Description
Governance and Ethical	• Robust Data Governance	• Ensuring that data is managed with confidentiality, integrity, and availability.
	• Data Classification, Management, and Storage	• Implementing systematic approaches to handle and secure data effectively.
	• Updated Technical Systems and Protocols	• Aligning technical systems with current best practices and standards.
	• Ethical Guidelines for Algorithmic Systems	• Establishing frameworks to ensure fairness, transparency, and accountability in algorithmic processes.
	• Transparency and Explainability	• Enhancing the clarity and comprehensibility of algorithmic decisions for all stakeholders.
Legal and Social Implications	• Solid Government Policies	• Developing and enforcing policies that effectively regulate algorithmic systems.
	• Collaborative Accord between Organizations	• Promoting cooperation among financial institutions, regulators, and other key stakeholders.
	• Digital Literacy Campaigns	• Educating the public on the implications and functioning of algorithmic systems.
	• Legal Support for Vulnerable Users	• Providing protections and resources to economically disadvantaged populations impacted by algorithmic decisions.

Table A2
Integrated IPA and AHP Methodology Employed in This Study

Step	Method	Description	Outcome
1	Data Collection	**IPA:** Conducted in-depth, semi-structured interviews with domain experts in finance, technology, and law.	Collected rich, qualitative data capturing experts' experiences, perceptions, and opinions related to GELSI in financial services.
2	Data Transcription	**IPA:** Transcribed each recorded interview verbatim to ensure accuracy and retain the authenticity of participants' responses.	Created a detailed, accurate record of each interview for further analysis.
3	Thematic Analysis	**IPA:** Systematically reviewed the transcriptions using thematic analysis to identify recurring patterns and themes relevant to the GELSI framework.	Identified key themes and patterns related to GELSI in the context of algorithmic systems.
4	Identification of Dimensions	**AHP:** Using literature reviews and expert opinions, identified dimensions from the GELSI framework to serve as decision criteria.	Established the key dimensions for evaluation in the GELSI framework based on thematic insights and expert opinions.
5	Pairwise Comparison & Ranking of Dimensions	**AHP:** Conducted pairwise comparisons of the identified GELSI dimensions, assigning relative importance scores to each dimension using multidimensional scaling based on expert interviews.	Produced a ranking of the GELSI dimensions by quantifying the relative importance of each criterion through comparison matrices.
6	Consistency Check	**AHP:** Calculated consistency ratios using the eigenvalue method to assess the reliability of expert judgments. A consistency ratio below 0.10 was deemed acceptable.	Ensured that expert judgments were consistent and reliable, validating the comparison matrices.
7	Determine Criteria Weights	**AHP:** Scored each dimension against the others and normalized the scores to identify the relative importance of each dimension. Using expert input, calculated each dimension's overall importance (or weight).	Quantified the relative significance of each criterion, providing priority weights for decision-making and creating a ranking for the GELSI framework dimensions.
8	Synthesis and Analysis	**IPA & AHP:** Synthesized the qualitative insights from IPA with the quantitative prioritization from AHP to create a comprehensive understanding of the key factors in algorithmic governance.	Developed a robust, actionable framework that integrates qualitative and quantitative findings, guiding recommendations for responsible algorithmic governance in finance.
9	Conclusion and Recommendations	**IPA & AHP:** Formulated informed conclusions and recommendations based on the integrated findings from both IPA and AHP, emphasizing the centrality of ethical guidelines, robust data governance, and coherent government policies.	Provided evidence-based recommendations for enhancing algorithmic governance in Indonesia's financial services, aligned with the GELSI framework.

Table A3
Findings and Illustrative Quotes on Governance and Ethical Dimensions

Finding	Description	Interview Excerpts
Proper and Robust Data Governance	Data governance is critical in the financial and fintech sectors, encompassing data protection and compliance with regulations.	**INV17**: "Since the 2022 Indonesian Personal Data Protection Law enactment, the finance industry has improved data governance, moving away from the previous chaos." **INV15**: "The issue is education. People often don't understand how their data is used, leading to misconceptions. Transparency is key, users need clear information about what data is collected and how it's used."
Confidentiality, Integrity, and Availability	The CIA triad is foundational for effective data governance, ensuring trust and operational effectiveness.	**INV9**: "Data is decrypted only for specific transactions and then re-encrypted. Access is highly restricted, with very few people in the company able to read the information."
Classification, Management, and Protection of Data	A comprehensive approach is necessary for data governance, covering all data lifecycle stages.	**INV11**: "Customers must fill out a form ensuring data confidentiality when applying for credit, and we follow strict ethical guidelines to protect their data." **INV8**: "Proper data governance is essential from data collection to its deletion."
Updated Technical Systems and Security Protocols	Maintaining cutting-edge technical infrastructure and security protocols is essential to remain competitive.	**INV11**: "We have a backup server for emergencies and have recently retrained our staff. We have also enhanced our security systems following a previous incident." **INV18**: "A fraud detection system (FDS) is essential for a Payment Service Provider to catch discrepancies, like suspicious transactions, that could go unnoticed."
Ethical Guidelines for Algorithmic Systems	Ethical guidelines tailored to algorithmic systems are necessary to harness their potential responsibly and prevent misuse.	**INV11**: "Associations like the fintech association should help craft the code of conduct through co-regulation. Relying solely on the law is not enough." **INV4**: "KORIKA aims to become an ethics association for AI, overseeing research and resolving disputes. However, we still have a long way to go in addressing ethical violations."
Transparency and Explainability in Algorithmic Systems Development Processes	Transparency and explainability in algorithmic systems ensure trust and alignment with societal values.	**INV3**: "There is a lack of transparency in how data is processed in Indonesia, unlike in other countries where users are notified about data recording. Users should have choices, but transparency is often missing. An independent organization is needed to oversee these processes." **INV3**: "Transparency in data processing is lacking. Users input data without knowing how it will be treated. Ideally, applications should be integrated to avoid multiple inputs." **INV6**: "There's a transparency issue in digital tools. While laws protect trade secrets, there needs to be a balance between ensuring security and protecting proprietary information."

Table A4
Findings and Illustrative Quotes on Legal and Social Implications Dimensions

Finding	Description	Interview Excerpts
Solid and Robust Government Regulation and Law Enforcement	Proactive government regulation and vigorous law enforcement are crucial for ethical algorithmic systems deployment.	**INV1**: "We lack the power to filter the influx of algorithmic systems products, leading to delayed regulations. The government should proactively establish minimal standards and a code of ethics for algorithmic systems governance." **INV16**: "Many laws and enforcement agencies already exist, but adequate supervision according to the established system is needed now." **INV17**: "Awareness is needed to protect personal data across private companies and government entities alike." **INV17**: "Personal data protection shouldn't be generalised, especially with algorithmic systems and blockchain. Law enforcement must be educated to handle these rapidly advancing technologies, ensuring they understand the responsibilities and obligations related to data breaches."
Collaborative Accord between Financial Bodies	Collaboration among financial stakeholders is essential for robust data governance and mitigating risks.	**INV13**: "We collaborate closely with compliance and legal teams and maintain strong ties with BI and OJK representatives to ensure we follow and understand the practical implementation of existing regulations."
Campaign to Promote Digital Literacy	Promoting digital literacy is vital to ensure users understand the digital landscape and navigate it safely.	**INV15**: "Regulations are stricter in the financial sector, but there's a lack of data literacy among users. This is partly because we, as professionals, make things too technical. Users need clear information on how their data is collected, used, controlled, and stored and its benefits."
Legal Support for Economically Disadvantaged Individuals	The effectiveness of data protection laws depends on their accessibility and fairness to all individuals.	**INV14**: "Due to unforeseen risks, regulations initially had to be stringent. However, we are now required to provide compensation despite our efforts in data security. This is part of UU PDP; previous regulations discussed similar provisions."

Table A5
Findings and Illustrative Quotes on Additional Emerging Dimensions

Finding	Description	Interview Excerpts
Additional Dimensions Emerge from Respondents	Additional key elements for managing algorithmic risk: implementing national/international standards (e.g., ISO), robust system design (BCP, DRP), algorithmic transparency and evaluation, quantifying data violation risks, leveraging resources (government, legal, and economic actors), enforcing compliance, and utilizing Regtech and Suptech for real-time monitoring.	**INV10**: "Risk management involves processes, frameworks, and procedures. I focus on ISO 31.000, but data governance in IT and finance is still underdeveloped. **INV18**: A Business Continuity Plan (BCP) is essential for handling data breaches or system failures. New data protection laws present challenges, particularly due to the risks of handling personal data." **INV15**: "Users need to be informed about the confidence levels of algorithmic systems' outputs. Expert consultation is still crucial for critical decisions. Public education is vital, especially in areas where algorithmic systems may give incorrect results, like rare diseases." **INV15**: "Continuous vigilance is crucial. Regular audits and evaluations of algorithm performance can help identify vulnerabilities and ensure algorithmic systems' reliability and accuracy. Detailed guidelines are needed to assess the severity of cybersecurity incidents and provide appropriate responses." **INV9**: "Both institutions could benefit from more technical expertise and a deeper understanding of risks. Collaborating with financial institutions is challenging, and more specialised experts are needed to manage algorithmic systems risks effectively." **INV6**: "Before the PDP law, enforcing data protection was difficult due to non-legal factors, even when laws and enforcement existed." **INV18**: "Digital Financial Innovation (DFI) emerged because BI and OJK couldn't manage the volume of digital innovations. Despite the high risks, Regtech and other innovations will continue evolving within regulatory sandboxes."

Appendix B

Using Analytic Hierarchy Process (AHP), we calculated criteria weights based on interviewees' evaluations of the GELSI framework dimensions. These weights quantify each dimension's relative importance in decision-making, ensuring objectivity in complex assessments. AHP employs a pairwise comparison matrix, systematically comparing dimensions based on perceived significance. In this process, a value of '1' on the diagonal signifies equal importance, while values greater than 1 indicate preference. For instance, a '3' at the intersection of Dimensions 4 and 6 suggests Dimension 4 is three times more critical than Dimension 6. Conversely, values between 0 and 1 (e.g., 1/3) indicate lower significance. If Dimension 6 scores 1/3 against Dimension 4, it holds only one-third of its importance. Larger values, such as '5', highlight greater preferences (e.g., Dimension 3 is five times more significant than Dimension 6). Table B1 presents the full comparison matrix.

Table B1
Pairwise Comparison Matrix for the Dimensions in the Proposed GELSI Framework

Dimension	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	3	3	3
2	1	1	1	1	1	1	1	1	1	3
3	1	1	1	1	1	5	1	3	1	3
4	1	1	1	1	1	3	1	3	1	3
5	1	1	1	1	1	3	3	3	1	3
6	1	1	1/5	1/3	1	1	3	3	1	3
7	1	1	1	1	1/3	1/3	1	3	3	3
8	1/3	1	1/3	1/3	1/3	1/3	1/3	1	1	3
9	1/3	1	1	1	1	1	1/3	1	1	3
10	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1/3	1

Based on the pairwise comparison matrix, the individual dimensions were contrasted based on importance. We then proceeded with further computation, where the matrix yielded specific numeric values indicating one dimension's relative significance over another. These values were normalized and synthesized to compute the final ranking percentages, as listed in Table 6. These percentages illustrate the priorities and weights for each dimension. A Consistency Index was derived to ensure the reliability of judgments. In this case, a consistency index of 8% indicated reasonable coherence and trustworthiness in the decision-making process. Table B2 presents the results of the AHP analysis.

Table B2
The rank of the Dimensions in the Proposed GELSI Framework based on AHP

No.	Dimensions	AHP Result	Consistency Index
1.	Proper and Robust Data Governance	0.124	0.08
2.	Confidentiality, Integrity, and Availability	0.1	
3.	Data Classification, Management, and Storage	0.134	
4.	Updated Technical Systems and Protocols	0.121	
5.	Ethical Guidelines for Algorithmic Systems	0.138	
6.	Transparency and Explainability	0.098	

(*continued on next page*)

Table B2 (*continued*)

No.	Dimensions	AHP Result	Consistency Index
7.	Solid and Robust Government Policies	0.111	
8.	Collaborative Accord between Organizations	0.056	
9.	Campaign to Promote Digital Literacy	0.086	
10.	Legal Support for Economically Disadvantaged Individuals	0.033	

The ten critical dimensions of the GELSI framework were ranked based on their importance in data governance and digital systems. The most crucial dimension was Ethical Guidelines for Algorithmic Systems (13.8%), followed by Data Classification, Management, and Storage (13.4%). Other high-priority dimensions included Proper and Robust Data Governance, Updated Technical Systems and Protocols, and Solid and Robust Government Policies. Conversely, Legal Support for Economically Disadvantaged Users (3.3%) and Collaborative Accord Between Organizations (5.6%) ranked the lowest. A consistency index of 8% ensured reliability and validity in rankings.

Proper and Robust Data Governance (Dimension 1) had the highest weight, emphasizing the need for clear protocols, security measures, and accessibility. Data Classification, Management, and Storage (Dimension 3) and Updated Technical Systems and Protocols (Dimension 4) also ranked highly, highlighting the importance of structured classification, secure storage, and technological updates for risk mitigation. Ethical Guidelines for Algorithmic Systems (Dimension 5) and Transparency and Explainability (Dimension 6) underscored the social implications of automated decision-making and the need for accountability. While Confidentiality, Integrity, and Availability (Dimension 2) ranked slightly lower, data protection remains fundamental. Solid Government Policies (Dimension 7) and Collaborative Efforts (Dimension 8) were significant but given less weight. Promoting Digital Literacy (Dimension 9) and Legal Support (Dimension 10) were the least prioritized but remain essential for inclusivity. These findings highlight the urgent need for ethical governance and strong data management in digital finance.

Data availability

Data will be made available on request.

References

Ahelegbey, D. F., Giudici, P., & Hadji-Misheva, B. (2019). Latent factor models for credit scoring in P2P systems. *Physica A: Statistical Mechanics and its Applications, 522*, 112–121. https://doi.org/10.1016/j.physa.2019.01.130

Ahmed, S., Alshater, M. M., Ammari, A. E., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. *Research in International Business and Finance, 61*, Article 101646. https://doi.org/10.1016/j.ribaf.2022.101646

Akter, S., McCarthy, G., Sajib, S., Michael, K., Dwivedi, Y. K., D'Ambra, J., et al. (2021). Algorithmic bias in data-driven innovation in the age of AI. *International Journal of Information Management, 60*, Article 102387. https://doi.org/10.1016/j.ijinfomgt.2021.102387

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability, 60*, Article 100989. https://doi.org/10.1016/j.jfs.2022.100989

Arnoldi, J. (2016). Computer algorithms, market manipulation and the institutionalization of high frequency trading. *Theory, Culture & Society, 33*, 29–52. https://doi.org/10.1177/0263276414566642

Arslan, A., Ahokangas, P., Haapanen, L., Golgeci, I., Tarba, S. Y., & Bazel-Shoham, O. (2022). Generational differences in organizational leaders: An interpretive phenomenological analysis of work meaningfulness in the nordic high-tech organizations. *Technological Forecasting and Social Change, 180*, Article 121717. https://doi.org/10.1016/j.techfore.2022.121717

Babaei, G., Giudici, P., & Raffinetti, E. (2025). A rank graduation box for SAFE AI. *Expert Systems with Applications, 259*, Article 125239. https://doi.org/10.1016/j.eswa.2024.125239

Bank Indonesia. (2021). *Bersinergi Mendorong Intermediasi, Mengakselerasi Pemulihan Ekonomi, Bank Indonesia*.

Bank Indonesia. (2023). *Dari visi menjadi realitas: Akselerasi transformasi digital menuju bank sentral DIgital terdepan untuk Indonesia maju*.

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Bartlett, R., Morse, A., Stanton, R., & Wallace, N. (2022). Consumer-lending discrimination in the FinTech era. *Journal of Financial Economics, 143*, 30–56. https://doi.org/10.1016/j.jfineco.2021.05.047

Bartneck, C., Lütge, C., Wagner, A., & Welsh, S. (2021). Privacy issues of AI, 61–70 https://doi.org/10.1007/978-3-030-51110-4_8.

Béland, D., & Howlett, M. (2016). The role and impact of the multiple-streams approach in comparative policy analysis. *Journal of Comparative Policy Analysis: Research and Practice, 18*, 221–227. https://doi.org/10.1080/13876988.2016.1174410

Belenguer, L. (2022). AI bias: Exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. *AI and Ethics, 2*, 771–787. https://doi.org/10.1007/s43681-022-00138-8

Boer, A., De Beer, L., & Van Praat, F. (2023). Algorithm assurance: Auditing applications of artificial intelligence. In E. Berghout, R. Fijneman, L. Hendriks, M. De Boer, & B.-J. Butijn (Eds.), *Advanced digital auditing* (pp. 149–183). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-11089-4_7.

Bollweg, L. M. (2022). *Data governance for managers*. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-65171-1

Brunelli, M. (2015). *Introduction to the analytic Hierarchy process*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-12502-2

Buhmann, A., & Fieseler, C. (2021). Towards a deliberative framework for responsible innovation in artificial intelligence. *Technology in Society, 64*, Article 101475. https://doi.org/10.1016/j.techsoc.2020.101475

Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2020). Explainable AI in fintech risk management. *Frontiers in Artificial Intelligence, 3*. https://doi.org/10.3389/frai.2020.00026

Cairney, P., & Jones, M. D. (2016). Kingdon's multiple streams approach: What is the empirical impact of this universal theory? *Policy Studies Journal, 44*, 37–58. https://doi.org/10.1111/psj.12111

Carlsson, V., & Rönnblom, M. (2022). From politics to ethics: Transformations in EU policies on digital technology. *Technology in Society, 71*, Article 102145. https://doi.org/10.1016/j.techsoc.2022.102145

Chang, T.-S., & Hsieh, Y.-C. (2024). Applying the analytic hierarchy process for investigating key indicators of responsible innovation in the Taiwan software service industry. *Technology in Society, 78*, Article 102690. https://doi.org/10.1016/j.techsoc.2024.102690

Chou, A. (2020). What's in the "black box"? Balancing financial inclusion and privacy in digital consumer lending. *Duke Law Journal, 69*, 1183–1217.

Coeckelbergh, M. (2018). Technology and the good society: A polemical essay on social ontology, political principles, and responsibility for technology. *Technology in Society, 52*, 4–9. https://doi.org/10.1016/j.techsoc.2016.12.002

Daim, T. U., & Dabić, M. (Eds.). (2023). *Cybersecurity: A technology landscape analysis*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-34843-3.

Danielsson, J. (2023). When artificial intelligence becomes a central banker. *VOX EU*. https://cepr.org/voxeu/columns/when-artificial-intelligence-becomes-central-banker.

Daníelsson, J., Macrae, R., & Uthemann, A. (2022). Artificial intelligence and systemic risk. *Journal of Banking & Finance, 140*, Article 106290. https://doi.org/10.1016/j.jbankfin.2021.106290

de Laat, P. B. (2018). Algorithmic decision-making based on machine learning from big data: Can transparency restore accountability? *Philosophy & Technology, 31*, 525–541. https://doi.org/10.1007/s13347-017-0293-z

Dignum, V. (2019). *Responsible artificial intelligence*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-30371-6

Dubber, M. D., Pasquale, F., & Das, S. (Eds.). (2020). *The oxford handbook of ethics of AI*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.001.0001.

Faghan, Y., Piazza, N., Behzadan, V., & Fathi, A. (2020). *Adversarial attacks on deep algorithmic trading policies*.

Fitsilis, F. (2019). *Imposing regulation on advanced algorithms*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-27979-0

Fletcher, G. G. S. (2021). Deterring algorithmic manipulation. In *Vanderbilt law review* (Vol. 259).

Floridi, L. (Ed.). (2021). *Ethics, governance, and policies in artificial intelligence*. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-81907-1.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., et al. (2021). An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, 19–39 https://doi.org/10.1007/978-3-030-81907-1_3.

Frei, C. (2023). Open banking: Opportunities and risks. In T. Walker, E. Nikbakht, & M. Kooli (Eds.), *The fintech disruption* (pp. 167–189). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-23069-1_7.

Ghioni, R., Taddeo, M., & Floridi, L. (2023). *Open source intelligence and AI: A systematic review of the GELSI literature*. AI & SOCIETY. https://doi.org/10.1007/s00146-023-01628-x

Giudici, P., Leach, T., & Pagnottoni, P. (2022). Libra or librae? Basket based stablecoins to mitigate foreign exchange volatility spillovers. *Finance Research Letters, 44*, Article 102054. https://doi.org/10.1016/j.frl.2021.102054

Giudici, P., & Raffinetti, E. (2023). SAFE artificial intelligence in finance. *Finance Research Letters, 56*, Article 104088. https://doi.org/10.1016/j.frl.2023.104088

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*, 220–265. https://doi.org/10.1080/07421222.2018.1440766

Gordon, G., Rieder, B., & Sileno, G. (2022). On mapping values in AI Governance. *Computer Law & Security Review, 46*, Article 105712. https://doi.org/10.1016/j.clsr.2022.105712

Gupta, R., Kukreja, G., Gupta, A., & Tyagi, L. (2021). Artificial intelligence fostering fintech: Emerging trends and use cases, 61–73 https://doi.org/10.1007/978-3-030-84842-2_5.

Hałaj, G., Martinez-Jaramillo, S., & Battiston, S. (2024). Financial stability through the lens of complex systems. *Journal of Financial Stability, 71*, Article 101228. https://doi.org/10.1016/j.jfs.2024.101228

Heriyanto, M. (2023). BI Akan perkuat keamanan siber sistem keuangan nasional. Antara https://www.antaranews.com/berita/3787782/bi-akan-perkuat-keamanan-siber-sistem-keuangan-nasional.

Hind, M. (2019). Explaining explainable AI, XRDS: Crossroads, the ACM magazine for students 25, 16–19 https://doi.org/10.1145/3313096.

Hoefer, R. (2022). The multiple streams framework: Understanding and applying the problems, policies, and politics approach. *J of Pol Practice & Research, 3*, 1–5. https://doi.org/10.1007/s42972-022-00049-2

Holford, W. D. (2022). 'Design-for-responsible' algorithmic decision-making systems: A question of ethical judgement and human meaningful control. *AI and Ethics, 2*, 827–836. https://doi.org/10.1007/s43681-022-00144-w

Hsu, J. (2022). *'Fair' AI looks at racial bias, New Scientist*.

Jacobs, J. (2023). How central banks are already deploying artificial intelligence. *The official monetary and financial institutions forum*.

Jalan, A., & Matkovskyy, R. (2023). Systemic risks in the cryptocurrency market: Evidence from the FTX collapse. *Finance Research Letters, 53*, Article 103670. https://doi.org/10.1016/j.frl.2023.103670

Jammalamadaka, K. R., & Itapu, S. (2022). Responsible AI in automated credit scoring systems, AI and Ethics. https://doi.org/10.1007/s43681-022-00175-3.

Johnson, G. M. (2021). Algorithmic bias: On the implicit biases of social technology. *Synthese, 198*, 9941–9961. https://doi.org/10.1007/s11229-020-02696-y

Jones, M. D., Peterson, H. L., Pierce, J. J., Herweg, N., Bernal, A., Lamberta Raney, H., et al. (2016). A river runs through it: A multiple streams meta-review. *Policy Studies Journal, 44*, 13–36. https://doi.org/10.1111/psj.12115

Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of big tech increasing in the policy process? The case of generative AI. *Policy and Society*. https://doi.org/10.1093/polsoc/puae012. puae012.

King, N. J., & Forder, J. (2016). Data analytics and consumer profiling : Finding appropriate privacy principles for discovered data. *Computer Law & Security Review, 32*, 696–714.

Kingdon, J. W. (2003). *Agendas, alternatives, and public policies* (2nd ed.). New York: Longman.

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy, 44*, Article 101976. https://doi.org/10.1016/j.telpol.2020.101976

Le Merrer, E., Pons, R., & Tredan, G. (2023). Algorithmic audits of algorithms, and the law, AI Ethics. https://doi.org/10.1007/s43681-023-00343-z.

Leitner, G., Singh, J., van der Kraaij, A., & Zsámboki, B. (2024). The rise of artificial intelligence: Benefits and risks for financial stability. *Financial Stability Review May*. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html.

Li, S., & Huang, Y. (2020). Do cryptocurrencies increase the systemic risk of the global financial market? *China and World Economy, 28*, 122–143. https://doi.org/10.1111/cwe.12314

Lin, Y.-T., Hung, T.-W., & Huang, L. T.-L. (2021). Engineering equity: How AI can help reduce the harm of implicit bias. *Philosophy & Technology, 34*, 65–90. https://doi.org/10.1007/s13347-020-00406-7

Mahanti, R. (2021). *Data governance and data management*. Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-3583-0

Maurer, T., & Nelson, A. (2021). *The global cyber threat*. International Monetary Fund.

Mirestean, A., Farias, A., Deodoro, J., Boukherouaa, E. B., AlAjmi, K., Iskender, E., et al. (2021). Powering the digital economy: Opportunities and risks of artificial intelligence in finance. *Departmental Papers, 2021*, 1. https://doi.org/10.5089/9781589063952.087

Morley, J., Machado, C. C. V., Burr, C., Cowls, J., Joshi, I., Taddeo, M., et al. (2020). The ethics of AI in health care: A mapping review. *Social Science & Medicine, 260*, Article 113172. https://doi.org/10.1016/j.socscimed.2020.113172

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics, 167*, 209–234. https://doi.org/10.1007/s10551-019-04407-1

Myers, M. D. (2013). *Qualitative research in business & management*. London: SAGE Publications Ltd.

Olszowski, R. (2024). Opening policymaking. In *Collective intelligence in open policymaking* (pp. 1–62). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-58191-5_1.

Omohundro, S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters, 1*, 19–21. https://doi.org/10.1145/2685328.2685334

Palladino, N. (2022). A 'biased' emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*. , Article 102479. https://doi.org/10.1016/j.telpol.2022.102479

Pedigoni Ponce, P. (2023). Direct and indirect discrimination applied to algorithmic systems: Reflections to Brazil. *Computer Law & Security Review, 48*, Article 105766. https://doi.org/10.1016/j.clsr.2022.105766

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT Professional, 17*, 32–39. https://doi.org/10.1109/MITP.2015.34

Polak, P., Nelischer, C., Guo, H., & Robertson, D. C. (2020). "Intelligent" finance and treasury management: What we can expect. *AI & Society, 35*, 715–726. https://doi.org/10.1007/s00146-019-00919-6

Powers, T. M., & Ganascia, J.-G. (2020). The ethics of the ethics of AI. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The oxford handbook of ethics of AI* (pp. 25–51). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190067397.013.2.

Pusparisa, Y. D. R. (2023). Governor of BI: Artificial intelligence changes the economic landscape. Kompas https://www.kompas.id/baca/english/2023/08/07/en-gubernur-bi-kecerdasan-buatan-mengubah-lanskap-ekonomi-indonesia.

Rachman, A. (2023). BI: Serangan siber ikut ganggu stabilitas sistem keuangan. *CNBC*. https://www.cnbcindonesia.com/market/20231023105516-17-482807/bi-serangan-siber-ikut-ganggu-stabilitas-sistem-keuangan.

Ruof, C. (2023). A reg- and suptech platform for fintech (policy proposal). In *Regulating financial innovation* (pp. 335–373). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-32971-5_10.

Sánchez, M. A., & De Batista, M. (2023). *Business continuity for times of vulnerability: Empirical evidence, contingencies & crisis mgmt* (Vol. 31, pp. 431–440). https://doi.org/10.1111/1468-5973.12449

Sargeant, H. (2023). Algorithmic decision-making in financial services: Economic and normative outcomes in consumer credit. *AI Ethics, 3*, 1295–1311. https://doi.org/10.1007/s43681-022-00236-7

Schwartz, M. J. (2015). *Hackers steal trading algorithms: Attacks aimed at hedge funds, trading firms, bank info security*.

Shinde, N., & Kulkarni, P. (2021). *Cyber incident response and planning: A flexible approach* (pp. 14–19). Computer Fraud & Security. https://doi.org/10.1016/S1361-3723(21)00009-9 (2021.

Silva, U. S. K. D., Paul, A., Hasan, K. W., Paul, S. K., Ali, S. M., & Chakrabortty, R. K. (2023). Examining risks and strategies for the spice processing supply chain in the context of an emerging economy. *IJOEM, 18*, 1124–1146. https://doi.org/10.1108/IJOEM-07-2020-0776

Smith, J. A., Flowers, P., & Larkin, M. (2009). *Interpretative phenomenological analysis: Theory, method and research*. London: Sage.

Stahl, B. C. (2021). Ethical issues of AI. In *Artificial intelligence for a better future* (pp. 35–53). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69978-9_4.

Strasser, A. (2022). Distributed responsibility in human–machine interactions. *AI and Ethics, 2*, 523–532. https://doi.org/10.1007/s43681-021-00109-5

Suhadolnik, N., Ueyama, J., & Da Silva, S. (2023). Machine learning for enhanced credit risk assessment: An empirical approach. *JRFM, 16*, 496. https://doi.org/10.3390/jrfm16120496

Švarc, J., Dabić, M., & Tekavčič, M. (2024). Controversies surrounding digitalization: Discussions in four key domains. In M. Dabić, J. Švarc, & T. U. Daim (Eds.), *Digital entrepreneurship in science, technology and innovation* (pp. 353–372). Edward Elgar Publishing. https://doi.org/10.4337/9781035311422.00022.

Svetlova, E. (2022). AI ethics and systemic risks in finance. *AI and Ethics, 2*, 713–725. https://doi.org/10.1007/s43681-021-00129-1

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1*, 557–560. https://doi.org/10.1038/s42256-019-0109-1

Tavana, M., Soltanifar, M., & Santos-Arteaga, F. J. (2023). Analytical hierarchy process: Revolution and evolution. *Annals of Operations Research, 326*, 879–907. https://doi.org/10.1007/s10479-021-04432-2

Theodorou, A., & Dignum, V. (2020). Towards ethical and socio-legal governance in AI. *Nature Machine Intelligence, 2*, 10–12. https://doi.org/10.1038/s42256-019-0136-y

Tracy, S. J. (2020). *Qualitative research methods: Collecting evidence, crafting analysis, communicating impact*. Wiley-Blackwell.

Tucker, C. (2019). Privacy, algorithms, and artificial intelligence. In A. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The economics of artificial intelligence: An agenda*. University of Chicago Press.

Violino, B. (2022). Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most. *CNBC*.

Vo, A., & Yost-Bremm, C. (2020). A high-frequency algorithmic trading strategy for cryptocurrency. *Journal of Computer Information Systems, 60*, 555–568. https://doi.org/10.1080/08874417.2018.1552090

Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly, 39*, Article 101685. https://doi.org/10.1016/j.giq.2022.101685

Xue, L., & Pang, Z. (2022). Ethical governance of artificial intelligence: An integrated analytical framework. *Journal of Digital Economy, 1*, 44–52. https://doi.org/10.1016/j.jdec.2022.08.003

Zahariadis, N. (2016). Delphic oracles: Ambiguity, institutions, and multiple streams. *Policy Sciences, 49*, 3–12. https://doi.org/10.1007/s11077-016-9243-3

Zhang, X., & Ding, Z. (2021). Multiscale systemic risk and its spillover effects in the cryptocurrency market. *Complexity, 2021*, Article 5581843. https://doi.org/10.1155/2021/5581843

Zhou, J., Chen, C., Li, L., Zhang, Z., & Zheng, X. (2022). FinBrain 2.0: When finance meets trustworthy AI. *Frontiers of Information Technology & Electronic Engineering, 23*, 1747–1764. https://doi.org/10.1631/FITEE.2200039

Zhu, T., Ye, D., Wang, W., Zhou, W., & Yu, P. (2021). More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2020.3014246, 1–1.

Arif Perdana's research, which covers a broad range of sectors such as finance, education, and healthcare, sheds light on the transformative power of digital technologies such as algorithmic systems, automated decision-making, data analytics, and blockchain. Through his studies, he has provided valuable insights into the challenges associated with adopting digital technologies and explored technology-driven strategies across various sectors. Currently, his research focuses on responsible artificial intelligence in finance, the applicability of blockchain in business, and machine learning algorithms. These diverse research interests showcase his comprehensive portfolio and dedication to tackling the intricate aspects of digital strategies.

As an Associate Professor at Monash University, Arif specializes in digital strategy, data science and analytics, and information systems management. He has been involved in academia for more than a decade, having worked at prestigious institutions such as the Singapore Institute of Technology, Aarhus University, and the University of Queensland. Before his academic career, Arif worked in the IT services and finance industries, giving him extensive experience in these sectors. Additionally, he serves as the Director of the Action Lab Research Network, Indonesia, Monash University since December 2022. Arif has been successful in securing substantial funding for his research, including grants from Singaporean institutions, Australian funding agencies, and the Indonesian government and corporations. Some notable research grants and projects include the Monash Data Future Institute (MDFI), Whyte Fund, Research Grant Bank Indonesia, and Singapore Institute of Technology Ignition Grants.

Saru Arifin is an associate professor at the Faculty of Law, Universitas Negeri Semarang, Indonesia. He earned a Ph.D. in human rights law from the Faculty of Law at the University of Pécs in Hungary. He is particularly interested in Public International Law, Human Rights Law, and Legislation Studies. He has published numerous articles in major international publications, including Routledge, Brill, and SAGE, which Scopus and WOS index. Furthermore, he is currently involved in academic organisations such as the Global Alliance for Justice Education (GAJE, USA) from 2019 to present, the Association for Asian Studies, the Indonesian Society of International Law (ISILL) from 2018 to present, the Asian Society of International Law from 2017 to 2018, and the Association for Border Studies from 2016 to 2017. He also serves as Director of Programs at the Institute for Migrant Rights in Cianjur, West Java, Indonesia, where he has worked since 2016. He was the Head of Law and Human Rights Advocacy Clinics from 2018 to 2020 and the Chief Editor of Pandecta: Research Law Journal from 2011 to 2020. From October 22, 2022, to February 21, 2023, he was a fellow at the Faculty of Social Science (FOSS) of Universitas Islam International Indonesia (UIII). Saru has been appointed as a member of the Ethical Committee for Academic Publishing within the Indonesian Law Journal Editors' Association (APJHI) for the year 2024 to 2029.

Novi Quadrianto is a professor of machine learning at the University of Sussex, UK. He holds a PhD in Machine Learning from the Australian National University and an undergraduate degree in Electrical and Electronics Engineering from Nanyang Technological University. Novi has international research experience in Finland, the United States, Canada, Germany, and Austria. He was a Newton International Fellow of the Royal Society at the University of Cambridge and has held prestigious positions at the Isaac Newton Institute for Mathematical Sciences and Wolfson College.

He has received several awards, including the 2023 Guarantor Researcher for BCAM Severo Ochoa Excellence Accreditation, the 2020 ELLIS Scholar/Fellow, the 2019 European Research Council ERC Starting Grant, and the 2012 N International Fellowship. Novi is an action editor for Transactions on Machine Learning Research and an associate editor for both the Frontiers in Big Data Journal and IEEE Transactions on Pattern Analysis and Machine Intelligence.