Volume 11 Issue 1 Year 2026 | Page 417-428 ISSN: 2527-9866
Received: ***25-01-2026*** | *Revised:* ***15-02-2026***| *Accepted:* ***27-02-2026***

Comprehensive Analysis: A Review of Loan Origination Systems from Information Systems and Regulatory Perspectives

R. Ali Fajar Saleh[1], Patah Herwanto[2], Harmansyah Nasution[2]
[1,2,3] Ekuitas University, Bandung, Indonesia, 40124
e-mail: september25.afs@gmail.com[1], pherwanto@ekuitas.ac.id[2], harmansyahnasution@yahoo.com[3]
*Correspondence: september25.afs@gmail.com

Abstract: *The Loan Origination System (LOS) has become a key infrastructure in Indonesia's digital mortgage lending ecosystem, where technological innovation increasingly intersects with regulatory governance. This study examines LOS through an integrated perspective that bridges information systems architecture and legal-regulatory frameworks. Using a qualitative normative-analytical approach grounded in systematic document analysis (2021–2026) and thematic synthesis, the research identifies a triple-layer compliance gap: a regulatory gap in technical specification, an implementation gap between regulatory intent and system design, and a legal defensibility gap concerning evidentiary robustness. The study proposes a conceptual legal-by-design framework integrating technical security, regulatory alignment, and evidentiary considerations within a unified architectural model. Rather than offering a validated industry standard, the framework serves as an analytical proposal to inform future empirical research and institutional system development.*

Keywords*: Loan Origination System; banking information systems; regulatory compliance; digital legal validity; mortgage lending.*

1. Introduction

Digital transformation has repositioned the Loan Origination System (LOS) as the core infrastructure of mortgage lending (Kredit Pemilikan Rumah/KPR) in Indonesia. Modern LOS platforms automate the loan lifecycle from application and credit scoring to approval and disbursement while increasingly integrating artificial intelligence, machine learning–based risk assessment, and real-time connectivity with OJK's Financial Information Service System (SLIK) (Sudianjaya & Yuhana, 2024) [1]. These developments mark a shift toward highly automated digital credit ecosystems. However, technological acceleration has outpaced regulatory harmonization. Information systems scholarship emphasizes architectural efficiency and analytics robustness [2], whereas legal frameworks impose obligations under Law No. 27 of 2022 on Personal Data Protection, the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 19 of 2016), and OJK Regulation No. 11/POJK.03/2022 on banking IT governance. Prior research in digital lending environments has identified emerging tensions between innovation and regulatory safeguards, particularly concerning borrower data protection [3].

Recent regulatory reforms such as OJK Regulation No. 40 of 2024 and OJK Circular Letter No. 19/SEOJK.06/2023 strengthen real-time integration and e-KYC requirements, while the full enforcement of the Personal Data Protection Law institutionalizes privacy-by-design principles. Yet evidence suggests that not all LOS implementations fully operationalize immutable audit trail requirements under Article 18(3) of OJK Regulation No. 11/2022, potentially weakening the evidentiary standing of digital credit transactions [4]. Additional uncertainty arises from the uneven adoption of accredited Electronic Certification Providers (PSrE), despite the formal recognition of electronic signatures under Article 11 of the Electronic Information and Transactions Law [5]. Supreme Court Decision No. 1234K/Pdt/2022 further underscores that admissibility of electronic evidence depends on demonstrable integrity and traceability.

This paper addresses these tensions by examining LOS through an integrated analytical perspective that bridges system architecture and regulatory governance. Drawing on regulatory document analysis (2021–2026), recent academic literature, and thematic gap analysis, the study proposes a conceptual triple-layer compliance model encompassing technical security, regulatory alignment, and legal defensibility. Rather than presenting a validated industry solution, the framework is offered as an analytical proposal to inform future empirical inquiry and institutional system design.

2. Literature Review

2.1 Conceptualizing the Loan Origination System in Information Systems Scholarship

Within information systems scholarship, the LOS has evolved from a back-office processing application into a strategic digital infrastructure shaping institutional competitiveness in financial services. Contemporary LOS platforms operate as integrated ecosystems automating the full lending lifecycle from digital onboarding and underwriting to approval and disbursement within real-time interconnected environments [6].

The technological development of LOS may be broadly categorized into three phases. First-generation systems (pre-2020) relied on fragmented modules that frequently generated data silos and inconsistent risk evaluation [2]. Second-generation systems (2020–2022) introduced partial integration with OJK's SLIK database and basic electronic Know-Your-Customer (e-KYC) functions supported by OCR, although critical verification processes often remained semi-manual [1]. Third-generation architectures (2023–present) incorporate artificial intelligence (AI) and machine learning (ML)–driven credit scoring, real-time API connectivity with regulatory infrastructures such as SLIK 2.0 and Pusdafil, and emerging blockchain-based mechanisms intended to enhance audit traceability [7].

Modern LOS architectures typically adopt microservices-based frameworks that enable modular scalability and resilience. Core functional components identified in recent studies include digital onboarding with liveness detection, data-driven credit engines integrating conventional and alternative datasets, workflow orchestration modules, encrypted document vaults, and compliance engines capable of automated regulatory checks [2], [6]. Empirical research associates digital LOS implementation with increased efficiency and improved credit governance outcomes [1], [8], [9], [10]. Nevertheless, several studies caution that fully immutable logging mechanisms are not yet consistently implemented, potentially exposing institutions to integrity and legal risks [1].

2.2 OJK's Regulatory Framework for Financial Technology and Housing Credit

Indonesia's regulatory framework governing digital lending operates across three interrelated domains: banking IT governance, fintech lending regulation, and cross-sectoral legal standards. OJK Regulation No. 11/POJK.03/2022 establishes the principal governance framework for IT implementation within commercial banks. Articles 16–20 mandate encryption standards, access control, and disaster recovery measures, while Article 18(3) requires immutable and user-traceable audit trails. Although normatively explicit, the regulation does not prescribe specific technological mechanisms, leaving flexibility in implementation. Existing analyses suggest that tamper-resistant logging such as blockchain-based or write-once-read-many (WORM) storage has not yet become standardized practice across the industry, indicating potential divergence between regulatory mandate and technological readiness. OJK Regulation No. 40/POJK.05/2024 further reshapes the digital lending landscape by strengthening e-KYC requirements in conjunction with OJK Circular Letter No. 19/SEOJK.06/2023, mandating active liveness detection aligned with ISO/IEC 30107 standards. The regulation also requires real-time integration with the Fintech Lending Data Center (Pusdafil), increasing architectural demands for API interoperability and system security [4].

Cross-sectoral legislation significantly influences LOS architecture. Law No. 27 of 2022 on Personal Data Protection institutionalizes purpose limitation and transparency principles, requiring granular consent management mechanisms. Concurrently, the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 19 of 2016) affirms the binding legal force of electronic signatures subject to requirements of authenticity, integrity, and exclusive control, thereby implying the use of certified Electronic Certification Providers (PSrE) rather than informal clickwrap mechanisms [11]. Collectively, these regulatory instruments form a multilayered compliance environment directly shaping digital mortgage system design.

2.3 Mortgage Documentation Standards and Digital Legal Validity

Mortgage lending in Indonesia remains anchored in prudential documentation standards derived from Bank Indonesia Circular Letter No. 12/38/DPNP of 2010, requiring borrower identification, financial capacity documentation, collateral certification, and insurance coverage. The digital transformation of these processes raises complex questions of legal validity. Ministerial Regulation of Agrarian Affairs/National Land Agency No. 1 of 2021 recognizes electronic land certificates as legally equivalent to physical certificates when verified through official systems. However, publicly documented API-level integration between banking LOS platforms and ATR/BPN verification systems remains limited, suggesting that semi-manual verification procedures may persist in practice.

While electronic signatures are legally recognized under Article 11 of the Electronic Information and Transactions Law, enforceability depends on compliance with certified provider requirements. Moreover, in transactions requiring authentic deeds particularly the Sale and Purchase Deed (Akta Jual Beli/AJB) Law No. 2 of 2014 on the Notary Profession continues to require in-person execution before authorized officials. Consequently, mortgage origination frequently operates under hybrid models combining digital processing with physical execution, limiting the realization of fully end-to-end digital transformation.

2.4 Research Gap: Bridging Architecture and Legal Defensibility

The literature on LOS remains divided between technical optimization studies and normative regulatory analyses. Information systems research focuses on architectural performance and predictive analytics [1], [6], whereas legal scholarship examines regulatory compliance and transaction validity [12]. Few studies systematically integrate these perspectives within a single analytical framework. Normative analyses of fintech regulation [4] demonstrate substantial consolidation of Indonesia's digital finance framework, yet they seldom address the architectural harmonization challenges arising from overlapping regulatory regimes banking IT governance, fintech-specific regulation, and personal data protection law. Tensions become particularly visible in the interaction between purpose limitation under the Personal Data Protection Law and AI-driven credit scoring models dependent on expansive datasets.

This intersection between regulatory obligation and system architecture constitutes the central research gap addressed in this study. By integrating technical compliance and legal defensibility within a unified analytical lens, the present research seeks to extend existing scholarship beyond isolated doctrinal or engineering approaches and toward a structurally coherent evaluation of digital mortgage systems.

3. Methods

3.1 Research Design

This study adopts a qualitative normative-analytical approach grounded in systematic document analysis and thematic synthesis. Rather than conducting empirical measurement or institutional auditing, the research examines the structural relationship between LOS architecture and Indonesia's evolving regulatory framework. The analysis integrates perspectives from

information systems and financial law, treating LOS as a socio-technical infrastructure operating within a regulated financial ecosystem. The objective is conceptual clarification and structural gap identification rather than statistical generalization. The resulting framework should therefore be interpreted as a theoretically grounded proposal intended to inform future empirical inquiry, not as a validated industry-wide model.

3.2 Data Sources

The study relies exclusively on documentary materials published between January 2021 and February 2026, grouped into three categories:

(1) Regulatory and Legal Documents

Primary materials were obtained from official repositories, including JDIH OJK and JDIHN, as well as relevant ministerial portals. These documents include OJK Regulations (POJK), OJK Circular Letters, statutory instruments governing personal data protection and electronic transactions, and ministerial regulations concerning electronic certificates and land administration. Revoked or non-relevant instruments were excluded to maintain doctrinal focus. The regulatory materials reviewed are summarized in Table 1.

Table 1. Regulatory and Legal Documents Reviewed in This Study (2021–2026)

Category	Source Repository	Scope of Review
OJK Regulations (POJK)	JDIH OJK	Banking IT governance, fintech lending, audit trail obligations
OJK Circular Letters	JDIH OJK	e-KYC, supervisory standards, cooling-off requirements
Statutory Instruments	JDIHN	Personal Data Protection Law, Electronic Information and Transactions Law
Ministerial Regulations	Official Ministry Portals	Electronic certificates, land administration
Industry Guidelines	Public institutional publications	Digital mortgage origination and compliance guidance

(2) Academic Literature

Peer-reviewed articles were identified through searches in Scopus, IEEE Xplore, Google Scholar, and Garuda using keywords such as “loan origination system,” “digital lending,” “electronic signature,” and “regulatory compliance.” Inclusion criteria were limited to publications (2021–2026) addressing digital lending architecture, regulatory governance, or legal validity within Indonesia or comparable ASEAN contexts. Non-peer-reviewed and promotional materials were excluded.

(3) Industry and Technical Standards

Selected technical standards including ISO/IEC 27001:2022, digital mortgage guidelines, and electronic certification frameworks were examined as normative reference points. These materials were not treated as empirical evidence but as technical benchmarks to contextualize regulatory interpretation.

3.3 Analytical Procedure

Analysis proceeded in three structured stages.

Stage 1: Regulatory Mapping. Each regulatory instrument particularly those issued by **Otoritas Jasa Keuangan** was systematically examined to identify the scope of obligation (such as audit trails, electronic know-your-customer (e-KYC), and consent requirements), its normative character (mandatory or advisory), the degree of technical specificity, and any cross-

references to other regulatory regimes. This stage aimed to assess the structural coherence and internal consistency of digital credit regulations, especially in relation to LOS architecture.

Stage 2: Comparative Standards Analysis. A requirement-mapping comparison was conducted across three domains: (1) conventional mortgage documentation standards, (2) digital lending guidelines, and (3) statutory requirements governing electronic transactions and data protection. The comparative focus centered on documentation validity, identity verification mechanisms, and logging or audit-trail obligations. The objective was to evaluate the extent to which formal legal mandates align with system architecture models and operational design principles in digital lending environments.

Stage 3: Thematic Synthesis. The findings were integrated through iterative thematic synthesis informed by directed content analysis. Four principal analytical themes emerged: (1) technical architecture and regulatory compliance, (2) legal validity of digital mortgage documentation, (3) data protection and consent governance, and (4) evidentiary robustness in dispute contexts. These themes structured the interpretative analysis and provided the foundation for the subsequent regulatory gap assessment.

Table 2. Thematic Categories Used in Document Analysis

Thematic Area	Conceptual Focus	Illustrative LOS Dimension
Technical Architecture	System design and structural integrity	Microservices, API integration, logging design
Data Governance	Lawful data processing principles	Consent management, purpose limitation
Legal Validity	Conditions of enforceability	Certified electronic signatures
Regulatory Alignment	Coherence with regulatory mandates	Reporting and IT governance obligations
Evidentiary Robustness	Capacity to withstand judicial scrutiny	Tamper-evident logs, metadata traceability

These categories function as qualitative analytical lenses rather than quantitative coding instruments.

3.4 Triple-Layer Gap Analysis Framework

Building on the thematic synthesis, the study applies a conceptual triple-layer gap framework to evaluate structural tensions in LOS implementation.

Table 3. Analytical Framework for Triple-Layer Compliance Assessment

Dimension	Guiding Question	Analytical Focus
Regulatory Gap	Do regulations provide sufficient operational clarity?	Normative precision and technical guidance
Implementation Gap	Do LOS architectures reflect regulatory intent?	Comparative interpretative alignment
Legal Defensibility Gap	Can digital transactions meet evidentiary standards?	Integrity, authenticity, traceability

The framework provides a structured qualitative lens integrating regulatory, architectural, and evidentiary dimensions. It does not employ numerical scoring.

3.5 Framework Development and Expert Consultation

The proposed LOS compliance framework was developed through iterative refinement based on the gap analysis. Informal expert consultation with academics and practitioners was conducted to assess conceptual coherence and practical plausibility. These consultations were exploratory and do not constitute formal validation.

3.6 Limitations
This study is limited to publicly available documents and literature. It does not include direct institutional audits or empirical compliance measurement. The jurisdictional focus on Indonesia further limits generalizability. Future research should incorporate case studies and system-level evaluations to assess operational applicability.

4. Results and Discussion
4.1 Regulatory Analysis of LOS: Normative Coherence and Technical Fragmentation
Analysis of 17 regulatory instruments (2021–2026) reveals a structural paradox in Indonesia's governance of Loan Origination Systems (LOS): strong normative coherence at the level of legal principles, yet technical fragmentation at the implementation level. Core instruments POJK 11/2022, POJK 40/2024, and Law No. 27/2022 on Personal Data Protection (PDP) align around three foundational principles: (1) protection of customer data, (2) transparency in credit decision-making, and (3) accountability through traceable audit trails. However, operational tensions emerge when these principles are translated into technical architecture. Three principal areas of regulatory friction are identified:

Data Minimization vs. Alternative Data Usage.
The PDP Law (Art. 20(1)) restricts data processing to specific purposes, while POJK 40/2024 implicitly encourages alternative data usage for credit scoring. POJK 11/2022 does not explicitly address minimization in banking IT governance. This divergence creates tension between predictive optimization and strict purpose limitation.

Immutability vs. Reversible Transaction States.
POJK 11/2022 (Art. 18) mandates immutable audit trails, whereas POJK 40/2024 introduces a 1×24-hour cooling-off period. Simultaneously, the PDP Law allows consent withdrawal. These provisions require architectural differentiation between immutable historical logs and temporarily reversible transaction states an engineering distinction not consistently implemented.

e-KYC Technical Standards.
POJK 40/2024 requires active liveness detection aligned with ISO/IEC 30107. The PDP Law mandates accurate identity verification but does not reference technical standards. This reflects limited formal harmonization between statutory norms and technical specifications. A central issue lies in Article 18(3) of POJK 11/2022, which mandates immutable audit trails without prescribing technical mechanisms (e.g., blockchain, WORM storage, or cryptographic controls). The absence of technical specification permits interpretive flexibility. In practice, conventional relational databases technically modifiable under elevated privileges remain in use. From an evidentiary perspective, integrity is a prerequisite for admissibility. Normative clarity without technical precision may therefore expose institutions to evidentiary vulnerability if transaction authenticity is challenged.

4.2 Integrating Information Systems and Legal Perspectives: Legal Validity of Digital Mortgage Documentation
Comparative analysis of three documentation regimes BI Circular Letter No. 12/38/DPNP (2010), AFTECH (2024) Digital Mortgage Guidelines, and ISO/IEC 27001:2022 reveals misalignment between conventional documentation standards and digital implementation models. Three categories illustrate this tension:

1) Digital Land Certificates
Ministerial Regulation No. 7/2016 recognizes electronic land certificates as legally equivalent, provided verification occurs through official systems. However, systematic API-level

integration between LOS platforms and ATR/BPN databases is not widely documented. Semi-manual verification methods (e.g., portal screenshots) remain observable, creating technical susceptibility to manipulation and potential title fraud risks.

2) Digital Credit Agreements

Article 11 of the Electronic Information and Transactions Law establishes four cumulative conditions for legally binding electronic signatures, reinforced by Government Regulation No. 71/2019 requiring certified providers (PSrE). Integration of certified services (e.g., PrivyID, VIDA) is not universal. Some LOS platforms rely on clickwrap or uncertified biometric signatures, which may weaken non-repudiation and evidentiary strength if challenged.

3) Deed of Sale and Purchase (AJB)

The AJB remains subject to in-person execution before a PPAT under notarial and land law frameworks. This statutory requirement prevents full end-to-end digitalization of mortgage origination. Digitally signed preliminary agreements may hold evidentiary value but do not replace the authentic deed requirement. Collectively, these findings demonstrate that legal validity in digital mortgage transactions depends on cross-regulatory coherence rather than single-regime compliance. Much of the information systems literature emphasizes efficiency and security, while cross-regime legal alignment remains underexplored.

4.3 The Triple-Layer Compliance Gap in LOS Implementation

Application of the three-dimensional gap analysis framework regulatory gap, implementation gap, and legal defensibility gap reveals three interrelated layers of vulnerability that may undermine the legal robustness of Loan Origination Systems.

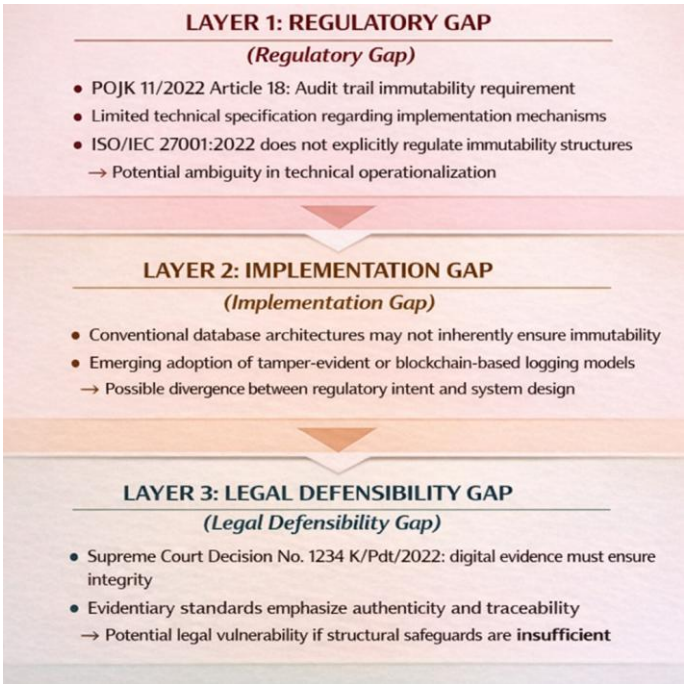

Figure 1. Triple-Layer Compliance Gap in the Architecture of the LOS

Particular attention to the third layer, the legal defensibility gap, exposes systemic risks that remain underexplored in information systems scholarship. In digital credit disputes, evidentiary rejection may stem not from factual inaccuracies in transaction data, but from the inability to demonstrate the integrity of electronic records. Judicial scrutiny frequently focuses on whether logging mechanisms are tamper-evident and capable of preserving the authenticity and completeness of digital evidence. Where systems lack cryptographically verifiable logging structures, the admissibility of electronic records may become vulnerable under judicial review.

This observation aligns with evidentiary principles embedded in the Electronic Information and Transactions Law, which require digital information to satisfy integrity and reliability standards when challenged in court. Legal scholarship on fintech governance further indicates that inconsistencies in metadata or system logs are typically uncovered through digital forensic audits rather than conventional internal monitoring mechanisms. In other words, vulnerability often becomes visible only when subjected to adversarial examination.

Existing studies on data protection in Indonesian digital transactions similarly highlight limitations in evidentiary safeguards, particularly concerning the demonstrable integrity of stored data. The emerging dimension, however, extends beyond privacy violations. Legal exposure may also arise from a system's inability to substantiate transactional integrity under forensic review. As AI-based credit scoring becomes increasingly sophisticated [17], [18], the demand for comprehensive audit trails grows correspondingly not only to validate transaction authenticity but also to demonstrate procedural transparency and algorithmic accountability. Yet, such forensic-oriented logging requirements remain largely underarticulated in current OJK regulations.

4.4 An Integrated Framework: Toward a Legal-by-Design Architecture for LOS

The preceding analysis indicates that vulnerabilities in Loan Origination System (LOS) implementation arise not from isolated technological or regulatory weaknesses, but from structural misalignment between normative mandates, architectural design, and evidentiary standards. To address this tension, this study proposes an Integrated LOS Compliance Framework grounded in the principle of *legal-by-design*, whereby regulatory obligations and evidentiary considerations are embedded at the architectural level rather than treated as post hoc compliance requirements. The framework is conceptual, derived from document synthesis and thematic integration. The structural configuration of the proposed architecture is illustrated in Figure 2.

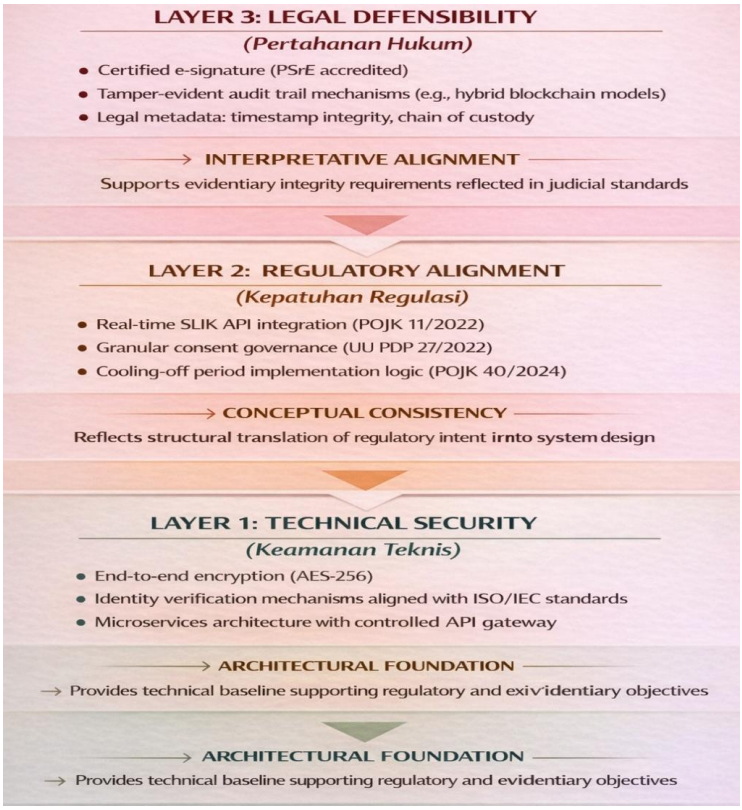

Figure 2. Conceptual Legal-by-Design Architecture for Loan Origination Systems

As depicted in Figure 2, the framework consists of three mutually reinforcing layers. The first layer, technical security, encompasses system integrity, encryption standards, logging mechanisms, and overall architectural resilience to ensure operational reliability and protection against unauthorized access or manipulation. The second layer, regulatory compliance, refers to alignment with banking IT governance requirements particularly those established by Otoritas Jasa Keuangan as well as fintech lending obligations and personal data protection regimes. The third layer, legal defensibility, concerns architectural mechanisms designed to enhance evidentiary robustness, ensuring that digital mortgage documentation and transaction records can withstand judicial scrutiny in dispute contexts. These three layers function as interdependent dimensions rather than as sequential stages of compliance, collectively forming an integrated governance architecture for digital lending systems.

(1) Structured Transaction-State Model

To reconcile the apparent tension between immutable audit trails and temporary transaction reversibility (e.g., cooling-off periods or consent withdrawal), the framework introduces a structured transaction-state model distinguishing:

- provisional state,
- confirmed state, and
- immutable archival state.

Immutability applies fully at the archival stage, while state transitions are preserved through tamper-evident logging. This distinction allows regulatory reversibility to coexist with historical traceability without undermining audit integrity. The model is presented as a conceptual architectural solution requiring empirical validation.

(2) Granular Consent Architecture

To address tension between data minimization and AI-based credit scoring, the framework proposes layered consent differentiation among:

- essential contractual data,
- alternative behavioral data, and
- third-party ecosystem data.

Withdrawal of non-essential consent does not automatically invalidate the underlying agreement, provided legally indispensable data remain intact. This mechanism conceptually reconciles predictive analytics with statutory purpose limitation, though practical implementation would require further regulatory clarification.

(3) Forensic-Oriented Audit Trail Design

The identified legal defensibility gap highlights the difficulty of demonstrating record integrity under judicial review. While regulations mandate immutability, they rarely specify forensic-level verification mechanisms.

The framework therefore advances a forensic-oriented audit architecture incorporating:

- cryptographic hash chaining,
- secure timestamping, and
- comprehensive metadata preservation.

This reframes audit trails from internal compliance tools into litigation-resilient structures capable of withstanding adversarial examination. The proposal is grounded in normative and jurisprudential analysis rather than institutional forensic testing.

Conceptual Contribution

The framework contributes analytically by conceptualizing legal defensibility as an architectural property of digital credit systems rather than a post hoc legal assessment. By integrating regulatory interpretation, documentation standards, and system design within a unified structure, it addresses a persistent gap in scholarship that often separates information systems optimization from legal validity analysis. Consistent with the study's methodological orientation, the framework should be understood as a theoretically grounded proposal. Empirical case studies, institutional audits, and longitudinal regulatory analysis are required to assess operational effectiveness in real-world banking and fintech environments.

4.5 Theoretical and Practical Implications

Theoretical Contribution

This study integrates information systems architecture with financial law analysis by conceptualizing legal defensibility as a system property. Legal validity emerges not merely from regulatory compliance but from architectural design anticipating evidentiary scrutiny. This extends compliance-by-design by incorporating a forensic dimension.

Practical Implications

The framework offers structured guidance for financial institutions seeking court-resilient LOS architecture. While advanced logging and cryptographic controls require greater investment, they conceptually reduce evidentiary risk. The transaction-state model provides a technical solution to reconcile immutability with cooling-off obligations. Regulatory implications are also evident. Greater technical specification comparable to international ICT risk management guidelines would enhance implementation clarity and reduce interpretive uncertainty.

5. Conclusions

This study examined the structural relationship between architecture and Indonesia's regulatory framework for digital mortgage lending. The analysis indicates a pattern of normative coherence at the regulatory level, contrasted with fragmentation in technical specification and system implementation. The findings suggest a triple-layer compliance gap comprising: (1) a regulatory gap in the translation of legal principles into operational technical standards; (2) an implementation gap between regulatory intent and prevailing system architectures; and (3) a legal defensibility gap concerning the evidentiary robustness of digital credit transactions.

In response, the study proposes a conceptual legal-by-design framework integrating technical security, regulatory alignment, and evidentiary considerations within a unified analytical structure. The framework is offered as a theoretically grounded proposal rather than a validated industry model. By reframing legal defensibility as an architectural property of digital financial systems, this study contributes to the integration of regulatory interpretation and system design analysis. Further empirical research is needed to assess the practical applicability of the proposed approach in institutional settings.

References

[1] A. Setyarko, E. R. Nugraha, T. A. Wibawa, and N. G. Dewi, "ENHANCING LOAN ORIGINATION THROUGH DIGITIZATION AND DATA ANALYTICS IN BANK BRI," *JAB*, vol. 10, no. 01, p. 68, Jun. 2024, doi: 10.47686/jab.v10i01.684.

[2] H. Nasution, A. Rahayu, L. A. Wibowo, P. D. Dirgantari, E. Yulianto, and R. Nurgraha, "Business Strategy Through SWOT Analysis in Implementing Loan Origination System to Improve Bank's Business Performance (Case Study at Mortgage Credit)," in *Proceedings of the 7th Global Conference on Business, Management, and Entrepreneurship (GCBME 2022)*, vol. 255, in Advances in Economics, Business and Management Research, vol. 255. , Dordrecht: Atlantis Press International BV, 2024, pp. 1593–1602. doi: 10.2991/978-94-6463-234-7_167.

[3] H. Agusta, "Perlindungan Data Pribadi Penerima Pinjaman Dalam Transaksi Pinjam Meminjam Uang Berbasis Teknologi Informasi (Peer to Peer Lending)," *krtha*, vol. 14, no. 2, pp. 163–192, Dec. 2020, doi: 10.31599/krtha.v14i2.189.

[4] A. Noor, D. Wulandari, and A.-S. Muhammad Afif, "Regulating Fintech Lending in Indonesia: A Study of Regulation of Financial Services Authority No. 10/POJK.05/2022," *QAJ*, vol. 3, no. 4, pp. 42–50, Oct. 2023, doi: 10.48161/qaj.v3n4a156.

[5] Triana Wati, "Kekuatan Hukum dan Aspek Keamanan Dalam Tanda Tangan Elektronik," *jssr*, vol. 1, no. 1, pp. 752–762, Oct. 2023, doi: 10.61722/jssr.v1i2.394.

[6] N. R. Sudianjaya and U. L. Yuhana, "DESIGN AND IMPLEMENTATION OF CENTRALIZED LOAN ORIGINATION SYSTEM WITH AGILE DEVELOPMENT METHOD," *IPTEK The Journal of Technology and Science*, vol. 35, Jul. 2024, [Online]. Available: https://iptek.its.ac.id/index.php/jts/article/download/17603/9026

[7] Narendra Bhargav Boggarapu, "Advanced cloud-based real-time credit scoring models: Leveraging big data and AI," *Int. J. Sci. Res. Arch.*, vol. 14, no. 1, pp. 988–995, Jan. 2025, doi: 10.30574/ijsra.2025.14.1.0112.

[8] H. P. Kothandapani, "Machine Learning for Enhancing Mortgage Origination Processes: Streamlining and Improving Efficiency," *int.jour.sci.res.mana*, vol. 8, no. 04, Apr. 2020, doi: 10.18535/ijsrm/v08i4.ec02.

[9] M. O. Kotb, "Credit Scoring Using Machine Learning Algorithms and Blockchain Technology," in *2023 Intelligent Methods, Systems, and Applications (IMSA)*, Giza, Egypt: IEEE, Jul. 2023, pp. 381–386. doi: 10.1109/IMSA58542.2023.10217411.

[10] N. Shirisha, Ch. Aswini, D. H. Reddy, J. Nagapuri, and G. P. Reddy, "MODERNISING LOAN APPROVAL: A DATA-DRIVEN APPROACH TO CREDIT DECISIONS," *JNAO*, vol. 14, no. 02, pp. 734–740, 2023, doi: 10.36893/JNAO.2023.V14I2.117.

[11] Rizqi Robi Ali Sodiqin, "Prinsip Jaminan Hukum Sebagai Jaminan Sertifikasi Tanda Tangan Elektronik," *Presidensial*, vol. 1, no. 2, pp. 13–23, Jun. 2024, doi: 10.62383/presidensial.v1i2.30.

[12] F. N. Buditama, I. W. Olii, and T. P. Azizah, "BATASAN PERTANGGUNGJAWABAN PPAT TERHADAP KETIDAKABSAHAN DOKUMEN KELENGKAPAN PERSYARATAN DALAM SISTEM HAK TANGGUNGAN ELEKTRONIK (HT-EL)," *JHCJ*, vol. 4, no. 1, pp. 31–50, Jun. 2024, doi: 10.30588/jhcj.v4i1.1839.

[13] D. W. Arner, J. N. Barberis, and R. P. Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm?," *SSRN Journal*, 2015, doi: 10.2139/ssrn.2676553.

[14] D. A. Zetzsche, R. P. Buckley, D. W. Arner, and J. N. Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation," *SSRN Journal*, 2017, doi: 10.2139/ssrn.3018534.

[15] H.-F. Hsieh and S. E. Shannon, "Three Approaches to Qualitative Content Analysis," *Qual Health Res*, vol. 15, no. 9, pp. 1277–1288, Nov. 2005, doi: 10.1177/1049732305276687.

[16] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006, doi: 10.1191/1478088706qp063oa.

[17] L. Adam *et al.*, "Driving Financial Inclusion in Indonesia with Innovative Credit Scoring," *JRFM*, vol. 18, no. 8, p. 442, Aug. 2025, doi: 10.3390/jrfm18080442.

[18] T. Wijaya, "The Rise of Innovative Credit Scoring System in Indonesia: Assessing Risks and Policy Challenges." CIPS, May 2023. [Online]. Available: https://repository.cips-indonesia.org/media/publications/560780-the-rise-of-innovative-credit-scoring-sy-3ee6d891.pdf