Journal of Trends in Finance and Economics
Print ISSN: 3007-6951
Online ISSN: 3007-696X
DOI: https://doi.org/10.61784/jtfe3077

DIGITAL GOVERNANCE OF FISCAL DEPOSITS IN LOCAL FINANCIAL INSTITUTIONS: A PROCESS-CONTROL FRAMEWORK

ShiYi Deng
Dublin International College, Beijing 100124, China.

Abstract: Fiscal deposits connect public cash management with the liquidity, compliance, and operational processes of local financial institutions. Their digitalization can improve visibility and execution speed, yet it can also amplify data inconsistency, automated control failure, cyber exposure, and accountability gaps when institutional rules and information architecture evolve at different rates. This paper develops a process-control framework for the digital governance of fiscal deposits in China. A structured qualitative synthesis of sixteen peer-reviewed studies, proceedings papers, and technical reports published mainly from 2018 to 2026 was combined with lifecycle analysis covering account authorization, fund placement, transaction execution, reconciliation, monitoring, and exit. The analysis identifies four interlocking deficiencies: fragmented process ownership, inconsistent data standards, reactive risk monitoring, and weak alignment between performance incentives and fiscal safety. In response, the paper proposes a four-layer framework integrating institutional authority, end-to-end process controls, governed data infrastructure, and continuous assurance. It further translates the framework into a risk-control matrix, measurable indicators, and a phased implementation roadmap. The main contribution is to move beyond isolated recommendations by showing how organizational responsibility, digital controls, and supervisory evidence can be linked at each stage of the fiscal-deposit lifecycle. The framework offers an implementable reference for fiscal authorities, local financial institutions, and financial supervisors seeking more transparent, efficient, and resilient deposit management.
Keywords: Fiscal deposits; Local financial institutions; Digital governance; Process control; Data governance; Risk monitoring

1 INTRODUCTION

Fiscal deposits are not ordinary commercial liabilities. They arise from the temporary custody, settlement, allocation, and safekeeping of public cash and therefore sit at the intersection of fiscal execution and banking operations. Their management affects cash visibility, payment continuity, institutional liquidity, interest allocation, compliance, and the quality of fiscal information. In local financial institutions, these functions are frequently distributed across treasury operations, corporate banking, accounting, information technology, compliance, and internal audit. The resulting arrangement creates a coupled system in which a weakness in account authorization or data exchange may propagate into reconciliation delays, inaccurate liquidity positions, or ineffective risk alerts. A recent conference paper identified defects in management systems and weak monitoring as persistent problems in local fiscal-deposit operations [1]. That diagnosis is important, but the accelerating digitalization of both fiscal platforms and banking processes requires a more integrated explanation of how such weaknesses arise and how controls should be redesigned.

Digital modernization can create substantial value. Integrated financial management information systems can automate transactions, reduce manual errors, improve reporting timeliness, and support cash planning. Recent technical guidance emphasizes that successful digital financial management depends simultaneously on functional design, information architecture, and governance capacity [2]. Modular system design is also preferable to a single monolithic replacement because core functions, institutional coverage, interfaces, and control requirements rarely mature at the same speed [3]. Evidence from information-system reforms shows, however, that technology acquisition alone does not produce better outcomes; institutional ownership, implementation sequencing, user capacity, and the quality of underlying processes are decisive [4]. These findings suggest that fiscal-deposit digitalization should be treated as a governance redesign rather than as an isolated software project.

The banking literature adds a second reason for caution. Digital transformation can improve information processing, management efficiency, and risk identification, but its effects are heterogeneous. Evidence from listed Chinese banks indicates that digitalization can reduce risk through improved profitability and operational capability [5], while other work finds reductions in systemic risk when digital transformation is supported by effective organizational mechanisms [6]. At the same time, digital expansion introduces new dependencies on data quality, automated rules, system availability, interface security, and model governance. Faster execution may therefore coexist with larger operational loss exposure or more rapid transmission of erroneous instructions. For fiscal deposits, the consequences are particularly material because the control objective is not limited to bank profitability; it also includes traceability, lawful use, liquidity availability, and verifiable stewardship of public cash.

Against this backdrop, the paper addresses three questions. First, which structural risks become most important when fiscal-deposit processes in local financial institutions are digitalized? Second, how can risks be mapped to preventive,

detective, and corrective controls across the deposit lifecycle? Third, which implementation sequence and performance indicators can convert a conceptual governance framework into an operational program? The study adopts a structured qualitative synthesis and institutional process analysis. It reviews sixteen core sources and codes their findings against lifecycle stages, risk mechanisms, control types, and accountable actors. The contribution is twofold. Conceptually, the paper combines public financial management, bank digitalization, data governance, and internal-control research within one process-control model. Practically, it provides a symmetric risk-control matrix and a staged roadmap that local institutions can adapt without assuming an immediate replacement of legacy systems.

The remainder of the paper is organized as follows. Section 2 reviews the relevant literature and establishes the analytical basis. Section 3 explains the research design and coding procedure. Section 4 diagnoses the principal risk dimensions and their interactions. Section 5 presents the proposed governance framework, control matrix, and implementation roadmap. Section 6 discusses theoretical and practical implications and acknowledges limitations. Section 7 concludes.

2 LITERATURE REVIEW AND ANALYTICAL BASIS

2.1 Fiscal Deposit Management as a Coupled System

Fiscal-deposit management includes the institutional and operational arrangements through which fiscal cash is authorized, placed, transferred, reconciled, monitored, and withdrawn from financial institutions. The object of control is therefore both a stock of cash and a stream of transactions. This distinction matters. Stock controls focus on account legality, balance visibility, concentration, and liquidity availability, whereas flow controls focus on instruction authenticity, payment timing, transaction purpose, exception handling, and reconciliation. A sound design must link the two. If account registers are incomplete, transaction-level analytics cannot establish a reliable population. If transaction interfaces lack common identifiers, aggregate balances may be visible while individual movements remain difficult to trace.

The direct literature on local fiscal deposits has mainly followed a problem-countermeasure structure. Cai describes weaknesses in management systems, monitoring, and coordination and proposes stronger rules and supervision [1]. This approach captures important institutional symptoms, yet it does not fully specify the control points, data objects, or feedback mechanisms needed in a digital environment. By contrast, financial management information-system research emphasizes architecture, modularity, interoperability, and implementation discipline [2-4]. Combining these streams suggests that fiscal-deposit governance should be modeled as a lifecycle with explicit control ownership rather than as a list of organizational shortcomings.

2.2 Digital Transformation and the Dual Effect on Risk

Digital transformation changes both the capacity to control risk and the channels through which risk emerges. Uddin et al. show that digital transformation can increase operational-risk exposure because expanded digital activity creates dependencies on systems, processes, and security controls [7]. Yin et al., however, find that digitalization can reduce operational risk when it improves the quality of internal control [8]. These results are not contradictory when control maturity is treated as a moderating condition: automation lowers error rates only when source data, rule logic, access rights, and exception escalation are reliable.

The same conditional logic appears in banking risk studies. Internal regulatory technology can mitigate credit risk by strengthening compliance applications and the technological foundation of control [9]. Economic uncertainty can alter the relationship between digital transformation and systemic risk through its effects on operational efficiency and profitability [10]. Other empirical studies report that digitalization changes systemic risk in the Chinese banking sector [11], and recent evidence warns that business and management digitalization may intensify systemic exposure through interbank activity and managerial incentives when external supervision and internal control are weak [12]. The general implication is that digitalization is not intrinsically risk-reducing. Its effect depends on the alignment between technology, incentives, organizational authority, and assurance.

2.3 Data Governance, Incentives, and the Research Gap

Data governance provides the connective tissue between institutional rules and automated controls. A broad review by Bernardo et al. identifies data ownership, quality management, assurance, and traceability as central capabilities across digital fields [13]. In fiscal-deposit management, these capabilities determine whether an account, instruction, balance, and reconciliation item can be represented consistently across fiscal and banking systems. Without a canonical data model and assigned data stewards, dashboards may display timely but semantically inconsistent information.

Incentives also shape outcomes. Digital investment may be profitable for banks [14], but a bank-level performance objective does not automatically coincide with fiscal objectives such as cash availability, transparent placement, and low concentration risk. Deposit competition can encourage balance-seeking behavior and contribute to financial fragility when incentives favor scale over risk-adjusted stewardship [15]. Dynamic digital capabilities are most productive when integrated with governance, risk management, and compliance rather than pursued as a standalone technology strategy [16]. Existing research therefore provides strong insights into separate components, but it lacks a

lifecycle-based framework that links fiscal authority, bank process ownership, data governance, control evidence, and measurable assurance. This paper addresses that gap.

3 RESEARCH DESIGN

3.1 Research Strategy and Evidence Base

The paper uses a structured qualitative synthesis combined with institutional process analysis. The approach is appropriate because the research objective is framework construction rather than causal estimation. The evidence base comprises sixteen core items: twelve peer-reviewed journal articles, three technical reports, and one conference paper. Publication dates range from 2018 to 2026 except that all sources fall within the ten-year window relevant to the target outlet. Sources were retained when they addressed at least one of four themes: fiscal-deposit or cash-management processes, financial management information systems, bank digital transformation and risk, or data and regulatory technology governance.

The selected literature was read against a common coding scheme. Each claim was assigned to a lifecycle stage, a primary risk mechanism, a control type, and an accountable actor. Preventive controls reduce the probability of an invalid event; detective controls identify deviations after or during processing; corrective controls restore an authorized state and preserve evidence. The coding also distinguished between institutional risk, process risk, data risk, and technology risk. Table 1 summarizes the evidence structure and its analytical use.

Table 1 Evidence Base and Analytical Use

Source type	Count	Primary focus	Use in this paper
Peer-reviewed journal articles	12	Bank digitalization, operational and systemic risk, data governance, profitability, and RegTech	Identify risk mechanisms, moderating conditions, and control capabilities
Technical reports	3	Financial management information systems, modular architecture, and reform implementation	Define architecture principles, sequencing, and implementation safeguards
Proceedings paper	1	Fiscal-deposit management in local financial institutions	Establish domain-specific problems and the baseline problem-countermeasure structure
Total	16	Publication window: 2018-2026	Structured coding by lifecycle stage, risk, control type, and accountable actor

3.2 Analytical Procedure

The analysis proceeded in four steps. First, the fiscal-deposit lifecycle was decomposed into six stages: account authorization, placement decision, transaction execution, intraday monitoring, reconciliation and reporting, and exit or renewal. Second, the literature was used to identify failure mechanisms at each stage, including unclear authority, inconsistent identifiers, manual intervention, delayed exceptions, weak incentive alignment, and technology concentration. Third, controls were matched to risks according to whether they prevent, detect, or correct a failure. Fourth, the controls were assembled into a layered architecture and tested for completeness using three questions: Does every material risk have an owner? Does every automated decision leave verifiable evidence? Can an exception be detected, escalated, resolved, and independently reviewed within a defined time?

The method does not assign numerical weights to risks because comparable institution-level data are not publicly available. Instead, it uses a traceable design logic: each proposed measure must correspond to a diagnosed risk, specify an implementing actor, produce an auditable output, and be assessable through at least one indicator. This constraint reduces the tendency of qualitative recommendations to remain general or disconnected from implementation.

4 CURRENT STATUS AND RISK DIAGNOSIS

4.1 Fragmented Process Ownership

The first risk dimension is fragmented ownership across the lifecycle. Fiscal authorities authorize cash arrangements, local financial institutions execute transactions and maintain accounts, supervisors assess compliance, and internal auditors evaluate control effectiveness. Within a bank, responsibility may be further divided among relationship management, operations, finance, information technology, compliance, and audit. When the responsibility map is not explicit, each unit may optimize its own task while no unit owns the end-to-end outcome.

Fragmentation appears in several forms. Account opening may satisfy bank onboarding requirements without being synchronized with a fiscal master register. Placement decisions may be approved through one channel, while transaction execution occurs through another. Reconciliation teams may identify exceptions but lack authority to suspend further activity. Technology teams may maintain interfaces without understanding the fiscal meaning of data fields. The result is an accountability gap: a transaction can pass each local checkpoint yet still fail the overall governance objective. Prior evidence concerning financial management systems consistently shows that unclear institutional ownership weakens the value of digital investment [2-4].

The consequences include duplicate or dormant accounts, delayed correction, inconsistent reporting, and control evidence distributed across systems. More importantly, fragmentation impairs incident response. If an abnormal transfer occurs, responsibility for validation, temporary restriction, fiscal notification, and evidence preservation may be contested. A digital platform can accelerate processing, but it cannot resolve ambiguous authority. Therefore, role design is a prerequisite for automation.

4.2 Inconsistent Data Standards and Limited Traceability

The second dimension concerns data consistency. Fiscal and banking platforms often use different account codes, organizational hierarchies, transaction descriptions, time stamps, and status definitions. Manual mapping tables may bridge these differences, but they introduce version-control problems and make lineage difficult to prove. A dashboard built on inconsistent master data can create an illusion of control while concealing classification errors.

Data-quality failures are especially damaging in reconciliation. A missing unique transaction identifier forces teams to match records using amount, date, and narrative fields. Such matching becomes unreliable when transactions are split, aggregated, reversed, or processed across reporting dates. Similarly, inconsistent definitions of available balance, ledger balance, and restricted balance can distort cash visibility. The data-governance literature emphasizes ownership, quality rules, metadata, and assurance as mutually reinforcing capabilities [13]. In fiscal-deposit operations, these capabilities should apply to both reference data and transaction data.

Traceability also depends on immutable evidence. Automated decisions should record the rule version, input data, time, operator or service identity, and resulting action. Without this record, an institution may know that an alert was generated but not why a transaction was classified as abnormal. Weak lineage limits auditability, model review, and dispute resolution. It also complicates cross-institution comparison because similar indicators may be calculated from different definitions.

4.3 Reactive Monitoring and Automation Risk

The third dimension is the persistence of reactive monitoring. Traditional review frequently relies on end-of-day or periodic reports. This approach may be adequate for stable, low-volume processes, but digital channels compress the time between instruction and settlement. By the time a periodic report identifies an exception, funds may have moved through several accounts or the relevant operational context may be lost.

Real-time monitoring is not a complete solution. Rule engines can generate excessive alerts if thresholds are not calibrated, causing staff to ignore low-value signals. Conversely, an overly narrow rule set may miss new patterns. Interfaces can fail silently, leaving the monitoring layer with incomplete data. Automated reconciliation may clear transactions that match on amount and date but differ in economic purpose. Digital transformation can therefore raise operational exposure when control design does not keep pace with business expansion [7], while strong internal-control quality can reverse this effect [8].

The principal issue is not whether automation should be used, but how it is governed. Rules require named owners, version control, test evidence, approval, monitoring of false positives and false negatives, and procedures for emergency suspension. Models require input-quality checks, explainable outputs, and human review for high-impact decisions. Service outages require fallback procedures that preserve authorization and evidence standards. Without these safeguards, automation replaces visible manual weakness with less visible technological dependence.

4.4 Misaligned Incentives and Incomplete Performance Measurement

The fourth dimension is incentive misalignment. Local financial institutions may value fiscal deposits as stable funding, relationship assets, or a basis for cross-selling. Fiscal authorities, by contrast, prioritize safety, liquidity, lawful use, service continuity, and transparent returns. If placement and staff evaluation focus mainly on deposit scale, price, or relationship growth, risk-adjusted stewardship receives insufficient weight. Deposit competition can influence bank behavior and contribute to fragility [15], while digital transformation may amplify scale-oriented incentives by making acquisition and transfer easier.

Existing scorecards often measure outputs rather than control quality. Deposit balances, transaction volumes, and interest outcomes are visible, whereas reconciliation aging, data defects, override frequency, concentration exposure, and incident closure are less prominent. This asymmetry encourages local optimization. A unit may meet its growth target while creating operational or liquidity risk elsewhere. Performance metrics should therefore connect business outcomes to control outcomes.

Incentive design also affects exception handling. Staff may hesitate to escalate a control failure if doing so delays a transaction or reduces reported performance. Automated overrides may become routine when operational targets are tight. The absence of consequences for repeated data-quality defects can transfer remediation costs to reconciliation and audit teams. A balanced scorecard should include timeliness, accuracy, concentration, control effectiveness, and remediation discipline, with clear thresholds for escalation.

4.5 Interaction Among the Risk Dimensions

The four dimensions reinforce one another. Fragmented ownership permits inconsistent data definitions to persist. Poor data quality weakens monitoring accuracy and produces alert fatigue. Reactive monitoring increases reliance on manual overrides, while scale-oriented incentives normalize those overrides. The resulting control environment is path dependent: each temporary workaround becomes embedded in later processes and system interfaces.

The critical bottleneck is the absence of a common control model that links authority, data, process, and assurance. Technology investment without such a model may improve local efficiency but increase system-wide opacity. Conversely, a purely institutional reform without digital evidence may be difficult to enforce at transaction speed. The appropriate response is therefore a layered framework in which institutional mandates define control objectives, processes operationalize them, data infrastructure makes them observable, and continuous assurance verifies their effectiveness.

5 PROCESS-CONTROL GOVERNANCE FRAMEWORK

5.1 Design Principles and Architecture

The proposed framework follows five principles. First, authority must precede automation: every account, rule, override, and exception requires an accountable owner. Second, controls should be embedded across the full lifecycle rather than concentrated at final review. Third, data should be governed as a shared control asset, with common identifiers, definitions, quality rules, and lineage. Fourth, automation must remain explainable and reversible for high-impact events. Fifth, assurance should be continuous, risk-based, and supported by measurable evidence.

Figure 1 presents the architecture. The institutional-authority layer defines mandates, risk appetite, segregation of duties, and escalation rights. The lifecycle-control layer embeds authorization, validation, limits, reconciliation, and closure procedures at each process stage. The governed-data layer provides master data, standardized messages, lineage, access logging, and quality monitoring. The continuous-assurance layer combines operational dashboards, compliance alerts, internal review, incident analysis, and periodic independent assessment. Feedback from assurance updates rules, data standards, and responsibility design.

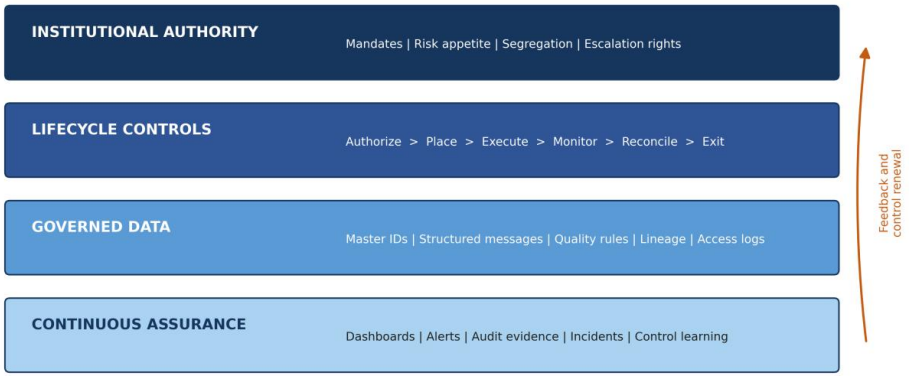

Figure 1 Layered Process-Control Architecture for Fiscal Deposits

The framework is deliberately modular. Institutions can begin with a verified account register and standardized reconciliation before implementing advanced analytics. This sequencing reflects the finding that modular financial management systems are easier to align with institutional capacity and that digital capability creates value when integrated with governance and compliance [3, 16].

5.2 Symmetric Risk-Control Matrix

Table 2 translates the four diagnosed dimensions into control packages. Each package includes preventive, detective, and corrective elements. This symmetry is essential: a policy statement without a detector cannot show whether it is followed, while a detector without a correction process merely records failure.

For fragmented ownership, the primary preventive control is a responsibility matrix approved jointly by fiscal and banking leadership. Each lifecycle stage should have one accountable owner, even where several units participate. Detective controls include overdue-action reports and unmatched handoffs. Corrective controls include escalation deadlines and post-incident responsibility reviews. The expected result is not the elimination of distributed work but the elimination of unowned outcomes.

For data inconsistency, the preventive controls are a canonical data dictionary, unique account and transaction identifiers, and controlled mapping between systems. Detective controls include automated completeness, validity, uniqueness, and consistency tests. Corrective controls route defects to named data stewards and require root-cause closure rather than repeated manual adjustment. Data-quality metrics should be reported with operational metrics, not confined to technology teams.

For reactive monitoring and automation risk, preventive controls include rule governance, pre-deployment testing, access segregation, and resilience design. Detective controls combine real-time alerts with monitoring of data-feed completeness, rule performance, and override frequency. Corrective controls provide transaction hold, controlled fallback, rule rollback, evidence preservation, and incident review. Internal RegTech research indicates that compliance-oriented technology can reduce risk when the underlying control foundation is strong [9].

For incentive misalignment, the preventive control is a balanced scorecard that weights safety, liquidity, compliance, and service quality alongside financial outcomes. Detective controls identify concentration breaches, repeated overrides, abnormal pricing, and discrepancies between reported performance and control quality. Corrective controls include adjustment of incentives, remediation plans, and restrictions on further placement until material weaknesses are addressed.

Table 2 Symmetric Risk-Control Matrix

Risk dimension	Preventive controls	Detective controls	Corrective controls	Lead owner and KPI
Fragmented ownership	Lifecycle responsibility matrix; segregation of duties; approved escalation rights	Overdue handoff report; unmatched ownership; approval-path review	Timed escalation; incident responsibility review; mandate revision	Joint process owner; unowned exception count; overdue action rate
Inconsistent data	Canonical dictionary; unique account and transaction IDs; controlled mappings	Completeness, validity, uniqueness, and cross-system consistency tests	Steward-led remediation; root-cause closure; controlled restatement	Data steward; first-pass reconciliation; defect recurrence
Reactive monitoring and automation risk	Rule ownership; pre-release testing; access segregation; resilience design	Real-time alerts; feed-health checks; false-positive and override monitoring	Transaction hold; fallback; rule rollback; evidence preservation	Operations and IT risk; alert age; override rate; recovery performance
Misaligned incentives	Balanced scorecard; concentration limits; risk-adjusted service criteria	Concentration alerts; abnormal pricing; repeated override and quality trends	Incentive adjustment; remediation plan; placement restriction	Business and compliance; concentration breaches; closure time

5.3 Governed Data Infrastructure and Continuous Assurance

The governed-data layer should be built around a small number of authoritative objects: institution, fiscal entity, account, mandate, transaction, balance, rule, alert, exception, and evidence item. Each object requires a unique identifier, owner, definition, effective date, source, and retention rule. Interfaces should transmit structured messages rather than free-text instructions wherever feasible. At ingestion, data should be checked for completeness, schema validity, duplication, time consistency, and authorization status.

Control evidence should be generated automatically. For example, an account-opening workflow should preserve approval identities, mandate scope, effective dates, and confirmation that the account is included in the master register. A placement workflow should preserve the approved criteria, concentration position, decision time, and execution confirmation. Reconciliation should link fiscal records, bank records, and adjustment evidence through the same transaction identifier. Every override should record reason, approver, duration, affected transactions, and subsequent review.

Continuous assurance does not mean that every transaction receives the same intensity of review. A risk-based engine can prioritize unusual amounts, new accounts, rapid movement, repeated reversals, late reconciliation, concentration changes, and activity outside expected time windows. High-risk alerts should be explainable and routed to staff with authority to act. The monitoring system should also evaluate itself through false-positive rate, missed-event review, data-feed availability, rule coverage, and time to closure. This meta-control prevents the monitoring layer from becoming an unexamined source of risk.

5.4 Implementation Roadmap and Performance Indicators

Table 3 Implementation Roadmap and Core Indicators

Phase	Time horizon	Priority actions	Exit evidence and indicators
Foundation	0-6 months	Map lifecycle; verify active accounts; assign owners; approve minimum data dictionary; establish baselines	Complete account register; ownership coverage; baseline reconciliation aging and defect rate
Integration	6-18 months	Standardize interfaces; automate reconciliation; deploy governed rules; connect exception workflow; test fallback	End-to-end ID coverage; first-pass reconciliation; alert acknowledgement; tested recovery
Optimization	18-36 months	Add advanced analytics; benchmark institutions; run scenarios; monitor controls continuously; refine incentives	Lower recurrence and override rates; improved closure time; stable data quality; risk-adjusted performance

Implementation should proceed in three phases, see Table 3. The foundation phase, covering approximately zero to six months, establishes governance prerequisites: lifecycle mapping, a verified account register, responsibility assignments, a minimum data dictionary, and baseline indicators. The integration phase, approximately six to eighteen months, standardizes interfaces, introduces automated reconciliation, deploys a controlled rules engine, and connects exception workflows. The optimization phase, approximately eighteen to thirty-six months, adds advanced analytics, cross-institution benchmarking, scenario testing, and continuous control monitoring.

Progress should be evaluated through a balanced set of indicators. Coverage indicators include the proportion of active accounts represented in the master register and the proportion of transactions carrying a unique end-to-end identifier. Quality indicators include first-pass reconciliation rate, unresolved data defects, and manual-adjustment frequency. Timeliness indicators include reconciliation aging, alert acknowledgement time, and incident closure time. Risk indicators include deposit concentration, override frequency, dormant-account count, and control failures by lifecycle stage. Resilience indicators include data-feed availability, recovery performance, and the completion rate of fallback tests.

Targets should be institution-specific and tightened after stable baselines are established. A universal threshold may create distorted behavior because transaction volume, system maturity, and account structures differ. Nevertheless, definitions must be common enough to support comparison. Each indicator should therefore specify a formula, owner, data source, frequency, tolerance, and escalation action. Independent review should verify both the reported value and the reliability of the underlying data.

6 DISCUSSION

The framework extends existing work in three ways. First, it treats fiscal-deposit management as a coupled lifecycle rather than as a static organizational function. This reveals how account design, transaction controls, data standards, and assurance depend on one another. Second, it reconciles conflicting findings on bank digitalization. Studies reporting risk reduction and studies reporting greater operational or systemic exposure can be interpreted through the moderating role of control maturity [5-8, 11-12]. Digitalization increases processing capacity; whether that capacity reduces or amplifies risk depends on governance, data quality, internal control, and incentive alignment. Third, the framework converts qualitative recommendations into observable control evidence and indicators.

The practical implication is that local financial institutions should not begin with advanced analytics. The highest-value first steps are a verified account population, clear lifecycle ownership, standardized identifiers, and disciplined reconciliation. These controls improve visibility and create reliable data for later automation. Fiscal authorities should define the control objectives and evidence requirements, while financial institutions should own execution, system controls, and operational remediation. Supervisors and internal auditors should test the design and effectiveness of the combined framework rather than reviewing isolated reports.

The framework also supports proportionality. Smaller institutions may implement the same control objectives with simpler technology, provided that authority, evidence, and escalation remain clear. Larger institutions require stronger segregation, real-time data-quality monitoring, and resilience testing because complexity and interconnectedness increase the consequences of failure. The modular structure avoids forcing all institutions into one technology architecture.

Several limitations should be acknowledged. The study is conceptual and does not estimate causal effects or validate indicator thresholds with institution-level transaction data. The evidence base combines public financial management and banking research because direct literature on digital fiscal-deposit operations remains limited. Institutional arrangements also vary across regions, which may affect the transferability of specific workflows. Future work should test the framework through comparative case studies, expert evaluation, process-mining data, and pilot implementations. Quantitative research could examine whether maturity scores predict reconciliation speed, incident rates, liquidity efficiency, or control failures.

7 CONCLUSION

This paper has examined how digitalization changes the governance requirements of fiscal deposits in local financial institutions. The analysis identifies four interlocking deficiencies: fragmented process ownership, inconsistent data standards, reactive monitoring with automation risk, and misaligned incentives. These deficiencies explain why technology can improve speed and visibility while simultaneously creating new forms of opacity and dependence.

To address the problem, the paper proposes a four-layer process-control framework integrating institutional authority, lifecycle controls, governed data infrastructure, and continuous assurance. The framework is operationalized through a symmetric risk-control matrix, a canonical set of data objects, measurable indicators, and a three-phase roadmap. Its central proposition is that digital value depends on control alignment: authority must be clear, data must be reliable, automated decisions must be explainable, and exceptions must lead to timely remediation.

The study contributes a structured bridge between fiscal cash management and bank digital-risk research. It also offers an adaptable implementation reference for fiscal authorities, local financial institutions, supervisors, and auditors. Future empirical work should validate the maturity model and estimate the relationship between control capability, operational performance, and fiscal-cash safety across different institutional settings.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Cai P. Analysis of issues and countermeasures in the management of fiscal deposits in local financial institutions. Proceedings of the 2025 7th International Conference on Economic Management and Model Engineering. Atlantis Press, 2026: 30-38. DOI: 10.2991/978-94-6239-602-9_4.
[2] Rivero del Paso L, Pattanayak S, Una G, et al. Digital solutions guidelines for public financial management. Washington, DC: International Monetary Fund, 2023. DOI: 10.5089/9798400251566.005.
[3] Una G, Allen R I, Botton N M. How to design a financial management information system: A modular approach. Washington, DC: International Monetary Fund, 2019. DOI: 10.5089/9781498311120.061.
[4] Hashim A, Piatti-Funfkirchen M. Lessons from reforming financial management information systems: A review of the evidence. World Bank Policy Research Working Paper 8312, 2018. DOI: 10.1596/1813-9450-8312.
[5] Chen Z, Li H, Wang T, et al. How digital transformation affects bank risk: Evidence from listed Chinese banks. Finance Research Letters, 2023, 58: 104319. DOI: 10.1016/j.frl.2023.104319.
[6] Yao T, Song L. Can digital transformation reduce bank systemic risk? Empirical evidence from listed banks in China. Economic Change and Restructuring, 2023, 56(6): 4445-4463. DOI: 10.1007/s10644-023-09560-2.
[7] Uddin M H, Mollah S, Islam N, et al. Does digital transformation matter for operational risk exposure? Technological Forecasting and Social Change, 2023, 197: 122919. DOI: 10.1016/j.techfore.2023.122919.
[8] Yin Q, Wang Y, Song D, et al. The impact of digitalization on operational risk: An organizational information processing perspective. International Journal of Production Economics, 2024, 276: 109369. DOI: 10.1016/j.ijpe.2024.109369.
[9] Shi Z, Xia Y, He L, et al. Can internal regulatory technology (RegTech) mitigate bank credit risk? Evidence from the banking sector in China. Research in International Business and Finance, 2025, 75: 102780. DOI: 10.1016/j.ribaf.2025.102780.
[10] He Y, Li W, Tan X, et al. Economic policy uncertainty, digital transformation, and bank systemic risk. International Review of Economics and Finance, 2025, 102: 104309. DOI: 10.1016/j.iref.2025.104309.
[11] Li Y, Xia Y, Sun Z, et al. Does digital transformation affect systemic risk? Evidence from the banking sector in China. International Review of Financial Analysis, 2025, 102: 104137. DOI: 10.1016/j.irfa.2025.104137.
[12] Huo W, Li J. Does digital transformation exacerbate systemic financial risks in banks? Evidence from listed commercial banks in China. Financial Innovation, 2026, 12: 107. DOI: 10.1186/s40854-026-00924-x.
[13] Bernardo B M V, Mamede H, Barroso J M P, et al. Data governance and quality management: Innovation and breakthroughs across different fields. Journal of Innovation and Knowledge, 2024, 9(4): 100598. DOI: 10.1016/j.jik.2024.100598.
[14] Citterio A, King T, Locatelli R. Is digital transformation profitable for banks? Evidence from Europe. Finance Research Letters, 2024, 70: 106269. DOI: 10.1016/j.frl.2024.106269.
[15] Acharya V V, Qian J, Su Y, et al. Fiscal stimulus, deposit competition, and the rise of shadow banking: Evidence from China. Management Science, 2025, 71(7): 5645-5675. DOI: 10.1287/mnsc.2023.04233.
[16] Abdurrahman A, Gustomo A, Prasetio E A. Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. The Electronic Journal of Information Systems in Developing Countries, 2024, 90(2): e12299. DOI: 10.1002/isd2.12299.