Future of Work and Digital Management Journal

Article type:
Original Research

Article history:
Received 27 August 2024
Revised 02 January 2025
Accepted 10 January 2025
Published online 01 March 2025

Providing a Model for Implementing an Effective Internal Control System in Banks

Abdulhamid Nazarian[1], Ali Saeedi[2*], Jafar Joola[3]

1 PhD student in Financial Engineering, Department of Financial Management, North Tehran Branch, Islamic Azad University, Tehran, Iran
2 Associate Professor, Department of Financial Management, North Tehran Branch, Islamic Azad University, Tehran, Iran

Corresponding author email address:
a_saeedi@iau-tnb.ac.ir

How to cite this article:
Nazarian, A.H. , Saeeidi , A. & Joola , J. (2025). Providing a Model for Implementing an Effective Internal Control System in Banks. *Future of Work and Digital Management Journal, 3*(1), 1-15. https://doi.org/10.61838/fwdmj.138

ABSTRACT

The purpose of this research was to propose a model for implementing an effective internal control system in banks. Accordingly, from the perspective of its objective, this is an applied study, because in addition to its informative and scientific aspects, it also has practical implications for various companies and organizations, especially banks. Considering the purpose and nature of the study, the research method is qualitative. Furthermore, since this research aims to design a model, it is exploratory in nature. The results showed that the final factors identified after the thematic analysis and data analysis stage include: organizational and structural barriers (deficiency in organizational structure, shortage of organizational resources, and weak organizational culture), legal and regulatory barriers (deficiency in laws and regulations, supervisory challenges, and compliance issues), technological and informational barriers (deficiency in technology infrastructure, information management challenges, and automation issues), human and skill-related barriers (lack of skills and knowledge, deficiency in training and development, and motivational and behavioral issues), process and operational barriers (deficiency in process design, implementation challenges, and supervision and control issues), and environmental and external barriers (economic impacts, competitive challenges, and technological and innovation influences).

Keywords: internal control implementation, bank, COSO, COBIT

Introduction

The insurance industry is undergoing a profound structural reconfiguration as digital technologies reshape risk discovery, pricing, distribution, claims, and even the institutional logic of intermediation. Under the umbrella of “InsurTech,” incumbent carriers and new entrants are assembling stacks that combine cloud-native architectures, data-intensive analytics, automation, and platform partnerships to deliver outcomes that are faster, more transparent, and—critically—more personalized across the policy lifecycle [1-3]. While the rhetoric of transformation is now ubiquitous, empirical and design-oriented research has begun to map the concrete levers that translate technology into measurable performance in insurance enterprises—innovation capability, digital operating models, and governance arrangements that balance agility with risk and compliance [4]. Against this backdrop, a feasibility-oriented model for “smart insurance” must take seriously not only the component technologies but also their orchestration into coherent processes and institutions that deliver value to customers, ecosystems, and regulators simultaneously.

Artificial intelligence and machine learning (AI/ML) are central to this reconfiguration because they convert heterogeneous data exhaust into predictive and prescriptive signals for underwriting, claims triage, fraud detection, retention, and cross-sell.

Recent syntheses show steep growth in AI/ML adoption across underwriting and claims, accompanied by new bibliometric clusters around explainability, fairness, and MLOps in insurance settings [5]. In parallel, practitioner research documents how big-data infrastructures and analytics pipelines extend the informational frontier, enabling carriers to ingest telematics, IoT device streams, geospatial imagery, and behavioral data for real-time decisioning [6]. The promise hinges on reliable data governance and model-risk management: models that are accurate in training but brittle in production can destroy value when claims volumes spike or when covariate shift undermines risk segmentation. Designing a smart insurance model therefore requires embedding AI/ML capabilities within resilient data platforms, model monitoring, and feedback loops—capabilities that our framework treats as separable but tightly coupled layers [1, 2].

A second pillar is distributed ledger technology and smart contracts, which reconfigure the contract layer itself. Concept and maturity assessments suggest that while blockchain is no panacea, there are well-defined use cases where shared, tamper-evident records and autonomous contract execution reduce reconciliation costs and accelerate claims—particularly in parametric products, reinsurance treaties, and multi-party processes [7]. Methodological work has specified how to implement blockchain-backed insurance for natural hazards, coupling oracles and event data with robust policy logic [8], while engineering studies show end-to-end solutions for parametric insurance in transport and logistics, where external data triggers automated indemnification under predefined conditions [9]. Architecture and governance remain decisive: aligning business process management (BPM) with on-chain logic clarifies roles, auditability, and exception handling [10], and cyber-insurance prototypes layering self-sovereign identity (SSI) on blockchain demonstrate privacy-preserving claims and credential flows [11]. More broadly, institutional analyses caution that enforceability, dispute resolution, and consumer protection must be designed around smart contracts to avoid shifting legal and operational risk to customers [12].

The sensorized world expands these opportunities and risks. IoT deployments in vehicles, homes, workplaces, and supply chains create continuous “evidence streams” that can price exposure dynamically, support loss prevention, and trigger automated claims; cloud–IoT reference models for integrated disaster management illustrate the operational patterns—ingest, detect, respond—needed when physical risk unfolds in real time [13]. At the same time, sector-specific models are emerging: for marine cargo, smart insurance concepts tie telemetry and workflow automation to coverage conditions [14]; for accidents, IoT-based detection and automated claim initiation have been prototyped with end-to-end paths from device to payout [15]. Smart home insurance has become a testbed for these ideas, with collaborative pricing schemes that require novel mechanism design to align insurer–insuree incentives while processing high-frequency device data [16]. Health insurance intensifies privacy, consent, and cybersecurity requirements; secure, technology-driven architectures and empirical validations demonstrate how confidentiality and integrity constraints can be embedded without blocking data-driven services [17]. Complementary security frameworks and reference designs for blockchain-based insurance emphasize authenticated data feeds, permissioning, and resilient contract upgrades as first-class design goals [18].

Digital transformation, however, is not only about components; it is an institutional process unevenly distributed across markets and lines of business. Country- and sector-level studies illustrate how policy, data infrastructure, and customer readiness shape adoption pathways. In China, post-pandemic acceleration brought remote distribution, digital claims, and ecosystem partnerships to the fore, with carriers reorganizing around platform logics and customer journeys rather than legacy product silos [19]. In rural development contexts, digital inclusive finance shows how data and mobile channels integrate primary, secondary, and tertiary industries, offering analogies for rural insurance distribution and agricultural risk

pooling [20]. Conversely, research on Bangladesh documents structural bottlenecks—digital identity coverage, literacy, regulatory clarity, and distribution fragmentation—that complicate the creation of digital insurance businesses, highlighting the need for staged capability building and policy coordination [21]. These contrasts suggest that feasibility models must be sensitive to institutional baselines: the same technical pattern will have divergent costs and benefits depending on market readiness and regulatory pragmatism [1, 2].

Climate and catastrophe risk sharpen the value proposition for automation and parametrics. Theories and evidence on climate-smart insurance indicate that timely payouts and risk-reduction incentives strengthen household and firm adaptive capacity, but only when contract design and distribution are tuned to local realities [22]. Multidisciplinary implementations for natural hazards show how event detection, oracle governance, and index calibration can make parametric contracts credible and scalable [8]. Ethical scrutiny is essential: smart information systems in insurance raise questions of opacity, surveillance, and fairness in pricing and claims decisioning; case studies urge proactive ethical governance and stakeholder engagement rather than retrofit controls after deployment [23]. Even product innovation trajectories—such as "smart product insurance," where coverage is embedded into connected devices—must anticipate consent management, dark patterns in app interfaces, and distributional impacts of risk-based pricing [24]. A feasibility model that centers organizational culture, change management, and stakeholder trust is therefore not a "soft" add-on but a core mitigant against technological and reputational risk [2, 3].

Market structure and ecosystem coordination further condition outcomes. Studies of insurer–tech collaboration highlight operating models in which incumbents open APIs, curate data marketplaces, and co-innovate with startups on narrowly scoped use cases before scaling [1]. In logistics and cargo, smart contracts knit together shippers, carriers, and insurers around verifiable milestones; empirical and engineering evidence shows both feasibility and the need for standardized data schemas and dispute pathways [9, 14]. In cyber insurance, architectures that combine on-chain credentials with off-chain analytics illustrate a path to lower friction and higher assurance across underwriting and claims [11]. More generally, redefining insurance through technology requires strategy choices about "where to play" (e.g., embedded distribution vs. stand-alone channels) and "how to win" (e.g., distinctive data assets, speed of model iteration, or experience-led service design) [2]. Bibliometric and synthesis work confirms that firms that link AI/ML capability building with process redesign and talent development realize more of the theoretical gains than those that layer models on unchanged workflows [4-6].

From a governance standpoint, the feasibility of "smart" models rests on codifying rules and responsibilities at the contract, process, and organizational levels. Business-process–aware smart contract frameworks align policy wording, underwriting authorities, claims adjudication, and audit requirements with programmable logic to reduce ambiguity and operational risk [10]. InChain-style architectures and secured insurance frameworks add identity, access control, and cryptographic assurances to the mix [11, 18]. IoT-heavy configurations, particularly in property and catastrophe domains, depend on resilient cloud backbones and well-specified incident response, as demonstrated in integrated disaster management patterns [13]. Because customers experience the service layer most directly, collaborative pricing and incentive design in smart home insurance show how insurers can co-produce risk reduction with policyholders, though not without addressing equity and behavioral responses [16]. Institutional commentary suggests regulators will increasingly scrutinize smart contracts' consumer outcomes, mandating explainability, recourse mechanisms, and defaults that protect vulnerable groups [12].

Strategic alignment with sustainability adds a further axis of feasibility. Green human resource management and green supply chain practices have been empirically linked to sustainable performance, implying that smart insurance programs should not only digitize but also "green" their operations and partner networks [25]. This resonates with environmental-risk products, where index-based or usage-based coverage aligns financial incentives with mitigation behaviors [8, 22]. At the same time, industrial and regional development agendas will push insurers to support digital inclusion—rural distribution, MSME enablement, and interoperable payment rails—consistent with evidence from inclusive finance contexts [20]. Taken together, these strands suggest that the feasibility of smart insurance is path-dependent: it emerges from reinforcing loops between technology maturity, process redesign, workforce skills, ecosystem standards, and public policy [1-3].

Finally, feasibility is an empirical question about fit: which capabilities, in what sequence, for which lines and segments? Research on the technology innovation level of insurance firms indicates that leadership commitment, cross-functional data teams, and investment in reusable platforms are strong predictors of InsurTech performance, but effects vary by market and by the orientation of partners and distributors [4, 19]. Case-led contributions across domains—parametric logistics, cyber identity, marine cargo, health, home, and disaster management—accumulate into a design space where smart contracts, AI/ML, IoT, and cloud are not buzzwords but configurable building blocks [9, 11, 13, 14, 16, 17]. Early conceptualizations of smart product insurance foreshadowed this embedded, data-rich future [24], and institutional analyses now chart the guardrails required to scale without eroding trust [7, 12, 23]. Building on this literature, the present study proposes and tests a comprehensive, multi-dimensional model that integrates technological, organizational, regulatory, market, and sustainability factors to assess and guide the establishment and implementation of smart insurance in practice.

Methodology

Considering the aim and nature of the study, this research is qualitative in method and was conducted through interviews with research experts. The study adopted a thematic analysis approach. The qualitative part of the research consisted of interviews with subject-matter experts; therefore, the statistical population included experts familiar with the research topic (university professors in the relevant field, supervisory staff of the banking network, and members of risk and audit committees within the banking system). In this part, theoretical sampling was used. In theoretical sampling, the focus is on sampling events rather than necessarily individuals; if individuals are approached, the primary goal remains exploring the events themselves.

Although there is no strict rule for sample size in qualitative research strategies, 6 to 8 units are suggested for homogeneous groups and 12 to 20 units for heterogeneous groups. The interviews continued until theoretical saturation was achieved. In this study, theoretical saturation was reached after interviewing 12 experts (university professors in the relevant field, supervisory staff of the banking network, and members of risk and audit committees within the banking system).

Sampling was carried out within the logic of qualitative methods and was purposive in nature. Two purposive sampling techniques were employed: purposeful sampling and snowball sampling. In qualitative research, purposeful sampling is commonly used to gather the most comprehensive and rich information; thus, the researcher selected participants who were considered "information-rich," meaning those who, based on the principles of qualitative research, could provide a strong and insightful picture of the phenomenon under study.

The core technique for the qualitative part of the study was thematic analysis, which was carried out using MAXQDA software.

Findings and Results

According to the results, 184 initial themes were categorized under 18 organizing themes. These organizing themes were then grouped into overarching global themes that represent the main categories of the research.

Table 1

Final Thematic Analysis Results

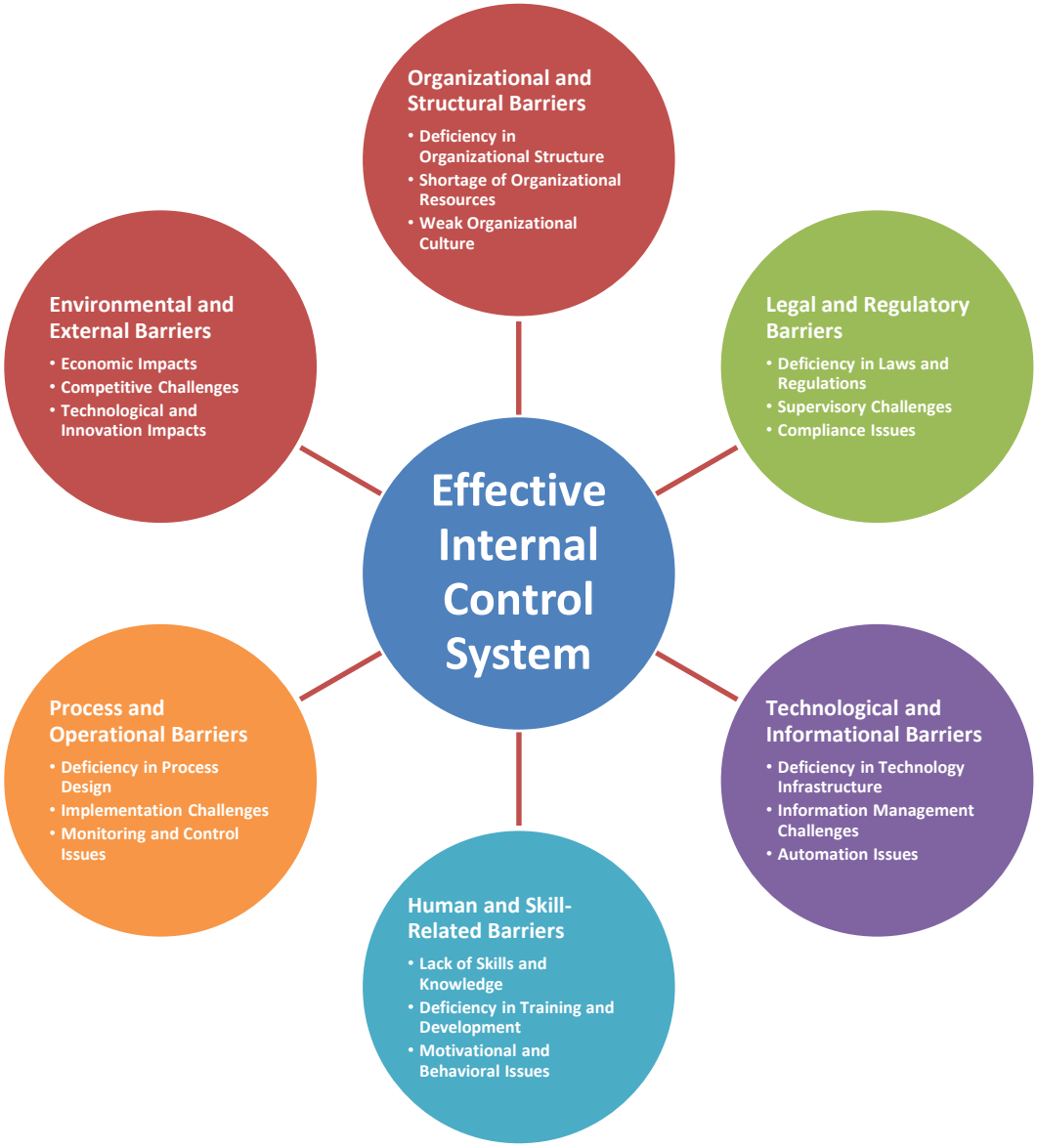
Initial Themes	Organizing Themes	Main Category
Improper segregation of duties	Deficiency in organizational structure	Organizational and Structural Barriers
Weakness in reporting hierarchy		
Lack of independent specialized committees		
Absence of a separate internal audit unit		
Overlapping authorities and responsibilities		
Weakness in defining job descriptions		
Lack of clear communication lines		
Non-independence of control units		
Weakness in corporate governance structure		
Deficiency in organizational formation		
Insufficient dedicated budget for internal control	Shortage of organizational resources	
Lack of specialized human resources		
Insufficient technical facilities and equipment		
Inadequate time allocation		
Deficiency in information resources		
Lack of adequate physical space		
No access to specialized software		
Lack of investment in infrastructure		
Shortage of training resources		
Absence of sustainable financing		
Lack of acceptance of internal control importance	Weak organizational culture	
Resistance to change		
Absence of responsibility culture		
Weak employee motivation		
Lack of top management commitment		
Absence of teamwork spirit		
Weakness in organizational communication		
Lack of transparency in performance		
Absence of continuous improvement culture		
Resistance to supervision		
Lack of comprehensive internal control laws	Deficiency in laws and regulations	Legal and Regulatory Barriers
Contradiction in existing regulations		
Lack of updated laws		
Absence of unified national standards		
Weakness in law enforcement		
Non-compliance with international standards		
Deficiency in executive guidelines		
Lack of clarity in law interpretation		
Absence of deterrent penalties		
Weakness in oversight of law enforcement		
Overlapping duties of supervisory bodies	Supervisory challenges	
Lack of coordination among supervisory bodies		
Weakness in supervisory capacity		
Lack of integrated supervisory approach		
Inadequate inspections		
Weakness in violation follow-up		
Absence of early warning systems		
No use of technology in supervision		
Weakness in supervisory reporting		
Lack of supervisory performance criteria		
Weakness in risk assessment	Compliance issues	

Non-compliance with international regulations		
Lack of compliance management system		
Weak oversight of compliance		
Lack of awareness of compliance requirements		
Deficiency in compliance documentation		
Failure to update compliance requirements		
Weakness in compliance reporting		
Absence of integrated systems	Deficiency in technology infrastructure	Technological and Informational Barriers
Obsolescence of existing systems		
Lack of adequate information security		
Weakness in data backup		
System incompatibility		
Deficiency in communication networks		
Lack of access to modern technologies		
Weakness in hardware infrastructure		
Absence of disaster recovery systems		
Insufficient bandwidth		
Data non-integration	Information management challenges	
Poor data quality		
Weakness in data accessibility		
Untimely information availability		
Lack of data standards		
Weakness in document management		
Insufficient protection of sensitive data		
Deficiency in information archiving		
Weakness in data analysis		
Lack of information sharing		
Lack of automation of control processes	Automation issues	
Deficiency in automated reporting systems		
Weakness in automated controls		
Non-integration of control systems		
Lack of continuous monitoring tools		
Weakness in automated control testing		
No automation for approval and authorization		
Deficiency in automatic transaction tracking		
Weakness in automated alerts		
Lack of automated reporting		
Lack of awareness of internal control standards	Lack of skills and knowledge	Human and Skill-Related Barriers
Deficiency in analytical skills		
Weakness in risk knowledge		
Lack of familiarity with modern technologies		
Absence of communication skills		
Weakness in managerial skills		
Insufficient knowledge of laws and regulations		
Deficiency in auditing skills		
Weakness in data analysis		
Lack of familiarity with best practices		
Absence of proper training programs	Deficiency in training and development	
Lack of continuous training		
Weakness in training needs assessment		
Lack of practical training		
Absence of specialized training		
Weakness in knowledge transfer		
Non-use of innovative training methods		
Deficiency in virtual training		
Weakness in training effectiveness evaluation		
Absence of international training		
Lack of employee motivation	Motivational and behavioral issues	
Deficiency in reward and punishment systems		
Weak job satisfaction		
Lack of organizational commitment		
Absence of responsibility sense		
Weakness in professional ethics		
Lack of active participation		
Deficiency in teamwork		
Weakness in responsibility acceptance		

Lack of willingness to learn		
Lack of process documentation	Deficiency in process design	Process and Operational Barriers
Deficiency in defining control processes		
Weakness in control points		
Non-integration of processes		
Absence of process standardization		
Weakness in process optimization		
Lack of process flexibility		
Deficiency in process sequencing		
Weakness in defining inputs and outputs		
Failure to update processes		
Inadequate implementation of controls	Implementation challenges	
Deficiency in monitoring execution		
Weakness in control testing		
Lack of continuous execution		
Absence of performance feedback		
Weakness in corrective actions		
Lack of proper follow-up		
Deficiency in performance reporting		
Weakness in effectiveness evaluation		
Lack of continuous improvement		
Absence of continuous supervision	Monitoring and control issues	
Deficiency in preventive controls		
Weakness in diagnostic controls		
Lack of corrective controls		
Absence of independent monitoring		
Weakness in risk evaluation		
Lack of change monitoring		
Deficiency in access controls		
Weakness in financial controls		
Lack of compliance oversight		
Inflation and economic instability	Economic impacts	Environmental and External Barriers
Economic uncertainty		
Decrease in investment		
Lack of integration in banking information systems		
Technical knowledge of bank managers		
Increased costs		
Decrease in revenues		
Impact of economic sanctions		
Lack of access to financial markets		
Intense competition in the banking industry	Competitive challenges	
Entry of new players		
Changing customer behavior		
Pressure to reduce costs		
Need for continuous innovation		
Change in business models		
Competition with FinTech companies		
Pressure on profit margins		
Changing customer expectations		
Need for competitive differentiation		
Speed of technological changes	Technological and innovation impacts	
Transparent reporting systems in banks		
Performance evaluation models of internal control in banks		
Use of advanced cybersecurity technologies in banks		
Financial process transparency in banks		
Emergence of disruptive technologies		
Complexity of banking processes		
Need to adapt to new technologies		
Cybersecurity threats		
Changing work patterns		
Need for new skills		
Technology costs		
System complexity		
Uncertainty regarding technology		
Rapid obsolescence of technology		

Figure 1

Final Thematic Analysis Model



Organizational and Structural Barriers: The results of the thematic analysis indicate that organizational and structural barriers are among the most critical challenges in implementing an effective internal control system in banks. This category comprises three main organizing themes: deficiency in organizational structure, shortage of organizational resources, and weak organizational culture. Deficiency in organizational structure, including issues such as improper segregation of duties, overlapping authorities and responsibilities, and lack of independence of control units, had the highest frequency in the interviews and highlights its critical importance from the experts' perspective. Shortage of organizational resources was also identified as a fundamental problem, including insufficient budget, lack of specialized human resources, and limited technical facilities. Weak organizational culture, manifested as resistance to change, lack of top management commitment, and absence of a culture of accountability, creates a foundation for failure in implementing internal control systems.

Legal and Regulatory Barriers: The legal and regulatory barriers category, which includes deficiency in laws and regulations, supervisory challenges, and compliance issues, underscores the importance of having a strong legal and regulatory framework to ensure the successful implementation of internal control systems. Deficiency in laws and regulations, reflected in the lack of comprehensive internal control laws, contradictions in existing regulations, and non-alignment with international standards, emerged as one of the key obstacles. Supervisory challenges, including overlapping responsibilities of supervisory bodies, lack of coordination among them, and weak supervisory capacity, hinder the effective enforcement of internal controls. Compliance issues, such as weak risk assessment, non-compliance with international regulations, and absence of a compliance management system, highlight the need for focused attention on compliance-related processes.

Technological and Informational Barriers: Technological and informational barriers, including deficiency in technology infrastructure, information management challenges, and automation issues, emphasize the critical role of information technology in the success of modern internal control systems. Deficiency in technology infrastructure, such as lack of integrated systems, outdated existing systems, and insufficient information security, emerged as one of the most significant barriers. Information management challenges, reflected in data non-integration, poor information quality, and limited accessibility of information, impede sound decision-making and effective control. Automation issues, such as lack of automation in control processes, weak automated controls, and deficiencies in automated reporting systems, reveal the necessity of enhancing the automation of control processes.

Human and Skill-Related Barriers: Human and skill-related barriers, including lack of skills and knowledge, deficiency in training and development, and motivational and behavioral issues, underscore the crucial role of human capital in the success of internal control systems. Lack of skills and knowledge, such as insufficient awareness of internal control standards, poor analytical skills, and weak risk knowledge, emerged as one of the key identified barriers. Deficiency in training and development, including the absence of proper training programs, lack of continuous training, and weak knowledge transfer, sustains skill-related challenges. Motivational and behavioral issues, manifested in lack of employee motivation, ineffective reward and punishment systems, and low job satisfaction, hinder active participation of employees in control processes.

Process and Operational Barriers: Process and operational barriers, including deficiency in process design, implementation challenges, and monitoring and control issues, highlight the importance of proper design and execution of control processes. Deficiency in process design, such as lack of process documentation, weak definition of control processes, and non-integration of processes, obstructs the creation of a coherent control system. Implementation challenges, including inadequate implementation of controls, poor supervision of execution, and weak control testing, reveal the gap between the design and execution of controls. Monitoring and control issues, such as lack of continuous supervision, deficiencies in preventive controls, and weakness in diagnostic controls, prevent timely detection of problems and effective corrective actions.

Environmental and External Barriers: Environmental and external barriers, including economic impacts, competitive challenges, and technological and innovation influences, demonstrate the effect of uncontrollable external factors on the establishment of internal control systems. Economic impacts, such as inflation and economic instability, economic uncertainty, and the effect of economic sanctions, create constraints on investment in internal control systems. Competitive challenges, including intense competition in the banking industry, entry of new players, and competition with FinTech

companies, put pressure on banks to reduce costs and improve efficiency. Technological and innovation influences, manifested in rapid technological changes, emergence of disruptive technologies, and cybersecurity threats, illustrate the necessity of continuously adapting internal control systems to dynamic environmental changes.

Discussion and Conclusion

The findings of this study provide a comprehensive understanding of the multidimensional barriers that hinder the effective establishment of internal control systems in banks. Through a rigorous qualitative approach and thematic analysis, six broad categories of obstacles were identified: organizational and structural barriers, legal and regulatory barriers, technological and informational barriers, human and skill-related barriers, process and operational barriers, and environmental and external barriers. These results deepen the theoretical understanding of how contextual, cultural, and technological factors converge to influence internal control effectiveness and align with and extend prior research.

A key contribution of this study lies in the identification of organizational and structural barriers as the most salient challenge to effective internal control systems. Issues such as improper segregation of duties, overlapping responsibilities, and lack of independence of control units emerged strongly. These findings support earlier research emphasizing that organizational design significantly affects control effectiveness and governance quality [26, 27]. Studies have consistently shown that unclear reporting lines and weak governance structures create control gaps that expose organizations to risk [28, 29]. Similarly, the shortage of dedicated financial and human resources reported in this study echoes previous evidence that resource limitations are a persistent obstacle to internal control maturity [30, 31]. Notably, the importance of organizational culture was also highlighted, with participants describing resistance to change and lack of top management commitment. This observation reinforces the argument that beyond technical frameworks, cultural readiness and ethical leadership are critical for sustaining effective internal controls [32, 33].

Another major insight is the role of legal and regulatory barriers, particularly the lack of comprehensive and up-to-date internal control laws, contradictory regulations, and weak supervisory mechanisms. These findings are consistent with prior research stressing the need for a robust regulatory foundation to support internal control frameworks [34, 35]. In many emerging financial systems, regulatory fragmentation and overlapping oversight responsibilities reduce enforcement capacity and create ambiguity in compliance [36, 37]. The participants' concerns about non-alignment with international standards reflect the challenges noted by [38] and [39], who emphasized that convergence toward global frameworks like COSO remains incomplete in developing contexts. Moreover, supervisory capacity gaps—such as insufficient risk-based oversight and absence of early warning mechanisms—mirror similar challenges reported in studies of local governments and public sector organizations [40, 41].

The study also underscores the profound impact of technological and informational barriers on internal control sustainability. Many banks still rely on fragmented, outdated IT infrastructures, weak information security, and non-integrated data systems. These findings align with [42] and [43], who argue that technological agility is now inseparable from control effectiveness. Digital innovations such as automated reporting, AI-driven analytics, and real-time monitoring can transform risk management, but their implementation is uneven across banking systems [44, 45]. Information management challenges—poor data quality, limited access, and weak document control—were also emphasized, echoing findings from

[31] and [39]. Additionally, the limited adoption of control automation identified in this study is consistent with the gap between technological potential and actual practice described in the literature [42, 46].

Human and skill-related barriers emerged as another critical factor limiting internal control performance. Interviewees pointed to insufficient awareness of control standards, weak analytical and risk management competencies, and lack of continuous training. These results confirm prior studies that highlight the pivotal role of human capital in sustaining governance systems [32, 33]. The absence of targeted and modern training initiatives parallels the observations by [28] and [47], who argue that without capacity building, technical frameworks like COSO and COBIT cannot be effectively institutionalized. Motivational and behavioral challenges such as low job satisfaction and weak reward systems also reflect the cultural and psychological dimensions of risk management [48]. When employees perceive internal control as punitive rather than enabling, engagement in control processes diminishes, leading to compliance gaps [49].

The findings regarding process and operational barriers—including poor documentation, non-standardized processes, weak control testing, and lack of continuous monitoring—further expand the understanding of why control systems often fail in practice. These results align with [34] and [50], who found that even when control frameworks exist, execution quality and operational discipline determine their impact on financial reporting accuracy. Continuous monitoring and timely corrective action, key elements of COSO's monitoring component, were notably underdeveloped in the studied banks, supporting [51]. The reported difficulties in bridging design and implementation reinforce the dynamic capability perspective suggested by [28], emphasizing the need for flexible and adaptive control practices rather than static checklists.

Finally, the study's identification of environmental and external barriers—economic instability, sanctions, competitive pressures, and rapid technological change—highlights the vulnerability of control systems to external shocks. These observations echo the macro-level constraints identified in [52, 53], showing how volatile economic conditions restrict investments in advanced control systems and long-term governance. Similarly, the intensifying competition from fintech disruptors places additional strain on banks to balance cost reduction and robust controls [54, 55]. Rapid technological obsolescence and cybersecurity threats further complicate efforts to maintain resilient systems [39, 42]. This suggests that internal control cannot be insulated from external market dynamics and must evolve within a broader risk management and strategic resilience perspective [32].

Taken together, the findings confirm and expand the multidimensional view of internal control effectiveness. The study builds on the foundational COSO framework [51] while demonstrating the necessity of contextual adaptation. It integrates structural, legal, technological, and cultural considerations to explain why theoretical best practices often fail to deliver in banking environments marked by uncertainty and rapid change. The results support a growing body of scholarship advocating for risk-based, technology-enabled, and culturally embedded control models [28, 29, 42].

Despite its comprehensive approach, this study has several limitations. First, it adopted a qualitative design based primarily on expert interviews; while this enabled deep exploration of context-specific challenges, it may limit the generalizability of findings to all banking environments. The sample, although theoretically saturated, was relatively small and drawn from a specific regulatory and cultural context, which could influence the types of barriers emphasized. Second, the study relied on participants' perceptions, which may carry subjective biases; triangulation with quantitative performance data or regulatory audits could have enhanced objectivity. Third, while the study examined a wide range of barriers, it did not measure the relative impact or prioritize them quantitatively, limiting actionable ranking for decision-makers. Finally, the fast-evolving

nature of banking technology and regulatory frameworks means that some identified issues—particularly technological and compliance-related—may shift rapidly, requiring continuous updating of the model.

Future research can address these limitations by adopting mixed-methods approaches that combine qualitative exploration with quantitative validation. For example, large-scale surveys or structural equation modeling could assess the relative weight of each barrier and examine their causal relationships with internal control performance metrics. Comparative cross-country studies could reveal how national regulatory maturity and economic stability shape the success of frameworks like COSO and COBIT in different banking contexts. Additionally, future studies should explore the integration of advanced analytics, AI, and blockchain in internal controls to understand their transformative impact on risk monitoring and compliance. Longitudinal research could track how banks adapt control systems over time in response to technological disruption and regulatory evolution. Exploring behavioral and psychological factors among employees, such as risk perception and control resistance, would also add depth to understanding cultural barriers.

Practitioners should focus on strengthening both the technical and cultural dimensions of internal control systems. Banks need to invest strategically in IT infrastructure, integrated data platforms, and automation to ensure real-time risk visibility and timely response. Top management must champion a risk-aware culture by clarifying roles, promoting accountability, and linking incentives to compliance and control objectives. Regulators and standard-setters should provide more consistent and harmonized frameworks to reduce ambiguity and support banks in adopting global standards while respecting local contexts. Continuous training and competency development for staff across all levels—particularly in analytics, cybersecurity, and compliance—are essential to sustain control effectiveness. Finally, banks should adopt dynamic, forward-looking risk management strategies that allow control systems to evolve alongside technological change and competitive market forces, ensuring resilience and trustworthiness in a volatile financial environment.

Acknowledgments

We would like to express our appreciation and gratitude to all those who cooperated in carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

The study protocol adhered to the principles outlined in the Helsinki Declaration, which provides guidelines for ethical research involving human participants. Written consent was obtained from all participants in the study.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

[1] S. Ahmad, R. Karim, N. Sultana, and R. P. Lima, "InsurTech: Digital Transformation of the Insurance Industry," in *Financial Landscape Transformation: Technological Disruptions*: Emerald Publishing Limited, 2025, pp. 287-299.

[2] S. Cosma and G. Rimo, "Redefining insurance through technology: Achievements and perspectives in InsurTech," *Research in International Business and Finance*, 2024, doi: 10.1016/j.ribaf.2024.102301.

[3] K. Balaji and E. Ariwa, "Insurtech disruption: Reshaping the future of insurance in the fintech era," in *The Adoption of FintechPB - Productivity Press*, 2024, pp. 247-266.

[4] J. Liu, Ye, Shujun, Zhang, Yujin, Zhang, Lulu, "Research on InsurTech and the technology innovation level of insurance enterprises," *Sustainability*, vol. 15, no. 11, p. 8617, 2023. [Online]. Available: https://www.mdpi.com/2071-1050/15/11/8617.

[5] P. Kumar, S. Taneja, E. Özen, and S. Singh, "Artificial Intelligence and Machine Learning in Insurance: A Bibliometric Analysis," pp. 191-202, 2023, doi: 10.1108/S1569-37592023000110A010.

[6] K. I. Jones and S. Sah, "The Implementation of Machine Learning In The Insurance Industry With Big Data Analytics," *International Journal of Data Informatics and Intelligent Computing*, vol. 2, no. 2, pp. 21-38, 2023, doi: 10.59461/ijdiic.v2i2.47.

[7] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?," *Future Internet*, vol. 10, no. 2, p. 20, 2018, doi: 10.3390/fi10020020.

[8] A. J. Pagano, F. Romagnoli, and E. Vannucci, "Implementation of blockchain technology in insurance contracts against natural hazards: a methodological multi-disciplinary approach," *Environmental and Climate Technologies*, vol. 23, no. 3, pp. 211-229, 2019, doi: 10.2478/rtuect-2019-0091.

[9] H. Dutta, S. Nagesh, J. Talluri, and P. Bhaumik, "A solution to blockchain smart contract based parametric transport and logistics insurance," *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3155-3167, 2023, doi: 10.1109/TSC.2023.3281516.

[10] A. Rachad, L. Gaiz, K. Bouragba, and M. Ouzzif, "A Smart Contract Architecture Framework for Insurance Industry Using Blockchain and Business Process Management Technology," *IEEE Engineering Management Review*, 2024, doi: 10.1109/EMR.2023.3348431.

[11] A. Farao, G. Paparis, S. Panda, E. Panaousis, A. Zarras, and C. Xenakis, "INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain," *International Journal of Information Security*, vol. 23, no. 1, pp. 347-371, 2024, doi: 10.1007/s10207-023-00741-8.

[12] L. D. Sotiropoulos, "Addressing Smart Contracts in the Insurance Sector: Institutional Framework and Practical Aspects," *ENTHA*, vol. 20, p. 22, 2023. [Online]. Available: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/entha20&section=9.

[13] S. Koduru, P. Reddy, and P. Padala, "Integrated disaster management and smart insurance using cloud and internet of things," *International Journal of Engineering & Technology*, vol. 7, no. 2.6, pp. 241-246, 2018, doi: 10.14419/ijet.v7i2.6.10777.

[14] C. B. Santoso, H. Prabowo, H. L. H. S. Warnars, and A. N. Fajar, "Smart Insurance System Model Concept for Marine Cargo Business," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 2021, pp. 281-286, doi: 10.1109/ICoDSA53588.2021.9617499.

[15] K. L. Narayanan, C. R. S. Ram, M. Subramanian, R. S. Krishnan, and Y. H. Robinson, "IoT based smart accident detection & insurance claiming system," in *2021 Third international conference on intelligent communication technologies and virtual mobile networks (ICICV)*, 2021, pp. 306-311, doi: 10.1109/ICICV50876.2021.9388430.

[16] D. Biswas and S. R. Vessal, "Smart home insurance: Collaboration and pricing," *European Journal of Operational Research*, vol. 314, no. 1, pp. 176-205, 2024, doi: 10.1016/j.ejor.2023.09.004.

[17] F. Al-Quayed, M. Humayun, and S. Tahir, "Towards a Secure Technology-Driven Architecture for Smart Health Insurance Systems: An Empirical Study," *Healthcare*, vol. 11, no. 16, p. 2257, 2023, doi: 10.3390/healthcare11162257.

[18] A. Hassan, M. I. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, and A. Alsufyani, "Secured insurance framework using blockchain and smart contract," *Scientific Programming*, vol. 2021, pp. 1-11, 2021, doi: 10.1155/2021/6787406.

[19] X. Xie, "Digital transformation trends of China's insurance industry after the COVID-19 pandemic," *Вестник Томского государственного университета. Экономика,* no. 54, pp. 228-238, 2021, doi: 10.17223/19988648/54/13.

[20] H. Ge, B. Li, D. Tang, H. Xu, and V. Boamah, "Research on digital inclusive finance promoting the integration of rural three-industry," *International Journal of Environmental Research and Public Health*, vol. 19, no. 6, p. 3363, 2022, doi: 10.3390/ijerph19063363.

[21] S. Rajput and S. Ahmad, "Challenges and Opportunities in Creating Digital Insurance Business in Bangladesh," *International Journal of Early Childhood Special Education*, vol. 14, no. 5, 2022. [Online]. Available: https://www.researchgate.net/profile/Suraiya-Rajput/publication/375282535_Challenges_and_Opportunities_in_Creating_Digital_Insurance_Business_in_Bangladesh/links/6545a690ce88b87031c2161b/Challenges-and-Opportunities-in-Creating-Digital-Insurance-Business-in-Bangladesh.pdf.

[22] B. Kramer and F. Ceballos, "Enhancing adaptive capacity through climate-smart insurance: Theory and evidence from India," 2018. [Online]. Available: https://ageconsearch.umn.edu/record/275926/.

[23] K. Natalija, "Insurance, smart information systems and ethics: A case study," *The ORBIT Journal*, vol. 2, no. 2, pp. 1-27, 2019, doi: 10.29297/orbit.v2i2.105.

[24] S. Ashraf and A. Zakaria, "Smart Product Insurance," 2020.

[25] A. A. Zaid, A. A. Jaaron, and A. T. Bon, "The impact of green human resource management and green supply chain management practices on sustainable performance: An empirical study," *Journal of Cleaner Production*, vol. 204, pp. 965-979, 2018, doi: 10.1016/j.jclepro.2018.09.062.

[26] S. M. Mortazavi and J. Shukrkhah, "Identifying Weaknesses in the Internal Control System of Iranian Banks," *Financial Accounting Research*, vol. 14, no. 1, pp. 81-108, 2022.

[27] A. Tahriri and S. Mohammadhosseinzadeh, "Identifying Factors Influencing the Establishment of an Internal Control System (Multiple Grounded Theory Approach)," *Accounting and Auditing Review*, vol. 29, no. 3, pp. 447-474, 2022.

[28] A. B. M. Metwally and A. Diab, "Towards an institutional understanding of risk-based management controls: evidence from a developing market," *Qualitative Research in Accounting & Management*, vol. 21, no. 2, pp. 165-191, 2024, doi: 10.1108/QRAM-05-2023-0087.

[29] N. N. Ma'rouf, "Presenting a Conceptual Model for Financial Internal Controls Based on Contingent Risks and Government Financial Reporting Transparency (Case Study: Kurdistan Regional Government of Iraq)," *Scientific-Research Quarterly of Accounting and Management Auditing Knowledge*, vol. 14, no. 3, pp. 279-297, 2025.

[30] A. Mizjat, M. R. Vatanparast, M. Moshkeli Miauqi, and K. Azadi, "Presenting an Internal Control System Model as a Mechanism for Enhancing the Quality Control of Banking Services," *Scientific-Research Quarterly of Accounting and Management Auditing Knowledge*, vol. 9, no. 36, 2020.

[31] S. I. Chang, L. M. Chang, and J. C. Liao, "Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach," *Information & Management*, vol. 57, no. 6, p. 103335, 2020, doi: 10.1016/j.im.2020.103335.

[32] L. Williams and P. Taylor, "Building a Risk-Aware Organizational Culture," *International Journal of Risk Management*, vol. 14, no. 1, pp. 45-60, 2023.

[33] P. Behbahani Nia and F. Orouji Kamalabad, "The Effect of Internal Control System Implementation on Financial Reporting Quality and Good Governance in Public Sector Organizations," *Auditing Knowledge*, vol. 23, no. 91, 2023.

[34] M. Dao, T. Pham, and H. Xu, "Internal control effectiveness and trade credit," *Review of Quantitative Finance and Accounting*, vol. 59, no. 4, pp. 1423-1452, 2022, doi: 10.1007/s11156-022-01079-3.

[35] V. Lakis and L. Giriūnas, "The concept of internal control system: Theorical aspect," *Journal of Accounting Literature*, vol. 42, pp. 80-103, 2022.

[36] K. Redeemer and M. Gerard, "Financial transparency, trust and willingness to pay in local governments of sub-Saharan Africa," *Journal of Public Budgeting, Accounting & Financial Management*, vol. 35, no. 6, pp. 100-120, 2023, doi: 10.1108/JPBAFM-06-2022-0110.

[37] F. Nanakweko, M. Kaur, and N. Rather, "Evaluating the impact of internal control systems on organizational effectiveness," *LBS Journal of Management & Research,* vol. 21, no. 1, pp. 135-154, 2023, doi: 10.1108/LBSJMR-11-2022-0078.

[38] A. Azinfar and E. Enayatpour Shiyadeh, "Globalization, a Challenge for Internal Control and Auditing in the Banking System," *Quarterly Journal of Accounting and Management Outlook,* vol. 4, no. 43, pp. 63-71, 2021.

[39] L. Christensen, "Internal audit: A case study of impact and quality of an internal control audit," *International Journal of Auditing,* 2022, doi: 10.1111/ijau.12280.

[40] M. Juma, N. David, and S. Muniru, "Determining the Relationship Between Internal Controls and Financial Accountability in Bushenyi District Local Government, Uganda," *Asian Journal of Economics Business and Accounting,* vol. 25, no. 3, pp. 328-336, 2025, doi: 10.9734/ajeba/2025/v25i31713.

[41] S. C. Drilia, "The Impact of Internal Control, HR Competence, and Organizational Commitment on Financial Report Quality Regional Government Organization, With IT Utilization as a Moderator (Study on Regional Government Organizations in Southern Sumatera)," *International Journal of Asian Business and Management,* vol. 4, no. 2, pp. 177-188, 2025, doi: 10.55927/ijabm.v4i2.155.

[42] G. Taylor and S. Green, "Advanced Monitoring Systems for Internal Control," *Global Business Insights,* vol. 48, no. 5, pp. 88-102, 2024.

[43] J. Smith and R. Brown, "The Role of AI in Enhancing Internal Controls," *Journal of Business Research,* vol. 45, no. 3, pp. 78-92, 2022.

[44] K. Yari Fard, "The COBIT Framework and Its Role as a Strategic Entity for the Management and Control of Information Technology Governance in Organizations," *Journal of New Achievements in Electrical, Computer, and Technology,* vol. 3, no. 6, pp. 38-55, 2023.

[45] A. Alfartoosi and M. A. Jusoh, "A conceptual model of e-accounting: Mediating effect of internal control system on the relationship between e-accounting and the performance in the small and medium enterprises," *International Journal of Economics and Management Systems,* vol. 6, pp. 228-252, 2021, doi: 10.33564/IJEAST.2021.v06i01.071.

[46] S. Yadegari, S. Ghoreshi, and E. Rajaeizadeh Harandi, "The Impact of Internal Control Quality on the Relationship Between Managerial Ability and Investment Efficiency in Companies Listed on the Tehran Stock Exchange," *Quarterly Journal of New Research Approach in Management and Accounting,* vol. 7, no. 88, pp. 43-60, 2023.

[47] C. Zalsa Bila Maulida Kemal and T. Tarjo, "The Impact of Internal Control Systems, Regional Financial Accounting Systems, and Information Technology Utilization on the Quality of Financial Reports in Local Government," *Apssai Accounting Review,* vol. 4, no. 2, pp. 143-151, 2024, doi: 10.26418/apssai.v4i2.103.

[48] H. Piri, M. Shahraki, H. Mottahedi, H. Rahat Dehmordeh, and R. Danesh, "Investigating the Degree of Management Ability's Impact on Internal Control Weaknesses in Listed Companies," *Journal of Applied Research in Management and Accounting,* vol. 9, pp. 33-20, 2024.

[49] N. A. Fatah, H. A. Hamad, and K. S. Qader, "The Role of Internal Audit on Financial Performance Under IIA Standards: A Survey Study of Selected Iraqi Banks," *Qalaai Zanist Journal,* vol. 6, no. 2, pp. 1028-1048, 2021, doi: 10.25212/lfu.qzj.6.2.38.

[50] C. S. Lennox and X. Wu, "Mandatory internal control audits, audit adjustments, and financial reporting quality: Evidence from China," *The Accounting Review,* vol. 97, no. 1, pp. 341-364, 2022, doi: 10.2308/TAR-2020-0152.

[51] C. Committee of Sponsoring Organizations of the Treadway, "Internal Control - Integrated Framework," 2020.

[52] A. Tamizi. "The effect of economic misery index on banks' financial performance." (accessed.

[53] F. S. Mahdi, A. S. Noorullah, and R. H. Jasim, "Supporting the internal control of banks with the methods of performance and financial intelligence to achieve leadership in business: An analytical study of a sample of Iraqi banks," *International Journal of Professional Business Review,* vol. 8, no. 2, 2023, doi: 10.26668/businessreview/2023.v8i2.1160.

[54] X. Zhang, F. Li, and J. Ortiz, "Internal risk governance and external capital regulation affecting bank risktaking and performance: Evidence from PR China," *International Review of Economics & Finance,* vol. 74, pp. 276-292, 2021, doi: 10.1016/j.iref.2021.03.008.

[55] S. Kashyap and E. Iveroth, "Transparency and accountability influences of regulation on risk control: the case of a Swedish bank," *Journal of Management and Governance,* vol. 25, no. 2, pp. 475-508, 2021, doi: 10.1007/s10997-020-09550-w.