INNOVATIONS IN TECHNOLOGY AND SCIENCE EDUCATION
ISSN 2181-371X
https://sr-journals.org/index.php/ITSE

Managing digital financial risks: the role of internal controls and governance structures

Axmadov Shukurbek Farruxovich
Student of the Faculty of Management at Tashkent State University of Economics
Email: shukurbekaxmadov@gmail.com

Abstract. The swift growth of the digital economy and advancements in financial technology have fundamentally altered how corporations operate, while also introducing digital financial risks, including cybersecurity threats, digital fraud, operational disruptions caused by algorithms, and systemic weaknesses. This paper examines the crucial role of internal control systems and corporate governance frameworks in mitigating these emerging risks. Using Agency Theory and the Dynamic Capabilities framework for analysis, the study investigates how traditional governance practices, including board oversight, audit committees, and compliance roles, must transition into ongoing, data-centric oversight structures that can guarantee organizational resilience. Through a conceptual-analytical lens, the study underscores the specific difficulties encountered by businesses in developing economies, where regulatory measures frequently fall behind digital advancements. The paper advocates for an Integrated Digital Governance Architecture (IDGA) that aligns the adoption of financial technologies with institutional security. The results indicate that effective governance serves not only as a means of compliance but also as a strategic factor in fostering long-term digital financial resilience.

Keywords: Digital financial risks, internal controls, corporate governance, emerging economies, Agency Theory, Dynamic Capabilities Theory, organizational resilience.

Annotatsiya. Raqamli iqtisodiyotning jadal rivojlanishi va moliyaviy texnologiyalardagi innovatsiyalar korporatsiyalar faoliyatini tubdan o‘zgartirdi, hamda shu bilan birga kiberxavfsizlik tahdidlari, raqamli firibgarlik, algoritmlar sababli yuzaga keladigan operatsion uzilishlar va tizimli zaifliklar kabi raqamli moliyaviy xavflarni keltirib chiqardi. Mazkur maqola ushbu yangi xavflarni kamaytirishda ichki nazorat tizimlari va korporativ boshqaruv mexanizmlarining muhim rolini tahlil qiladi. Tadqiqot Agentlik nazariyasi (Agency Theory) hamda Dinamik qobiliyatlar (Dynamic Capabilities) konsepsiyalariga tayangan holda, direktorlar kengashi nazorati, audit qo‘mitalari va komplayens funksiyalari kabi an’anaviy boshqaruv amaliyotlari tashkilot barqarorligini ta’minlay oladigan uzluksiz va ma’lumotlarga asoslangan nazorat tizimlariga aylanishi zarurligini o‘rganadi. Konseptual-tahliliy yondashuv asosida tadqiqot, ayniqsa, rivojlanayotgan davlatlardagi kompaniyalar duch kelayotgan muammolarni yoritadi, chunki bu mamlakatlarda tartibga soluvchi mexanizmlar ko‘pincha raqamli innovatsiyalar sur’atidan ortda qoladi. Maqolada moliyaviy texnologiyalarni joriy etishni institutsional xavfsizlik bilan uyg‘unlashtiruvchi Integratsiyalashgan Raqamli Boshqaruv Arxitekturasi (Integrated Digital Governance Architecture – IDGA) modeli taklif etiladi. Tadqiqot natijalari samarali boshqaruv nafaqat muvofiqlikni ta’minlash vositasi, balki uzoq muddatli raqamli moliyaviy barqarorlikni shakllantiruvchi strategik omil ekanini ko‘rsatadi.

Kalit so‘zlar: Raqamli moliyaviy risklar, ichki nazorat tizimlari, korporativ boshqaruv, rivojlanayotgan mamlakatlar, Agentlik nazaroyasi (Agency Theory), Dinamik qobiliyatlar nazariyasi (Dynamic Capabilities Theory), tashkiliy barqarorlik.

Аннотация: Стремительное развитие цифровой экономики и инновации в сфере финансовых технологий коренным образом изменили деятельность корпораций, одновременно породив новые цифровые финансовые риски, включая угрозы кибербезопасности, цифровое мошенничество, операционные сбои, вызванные алгоритмами, а также системные уязвимости. В данной статье рассматривается ключевая роль систем внутреннего контроля и механизмов корпоративного управления в снижении этих

возникающих рисков. Опираясь на Теорию агентских отношений (Agency Theory) и концепцию динамических способностей (Dynamic Capabilities Theory), исследование анализирует, каким образом традиционные практики управления, включая контроль со стороны совета директоров, деятельность аудиторских комитетов и функции комплаенса, должны трансформироваться в непрерывные, ориентированные на данные структуры надзора, способные обеспечивать организационную устойчивость. На основе концептуально-аналитического подхода в исследовании подчеркиваются специфические трудности, с которыми сталкиваются компании в развивающихся экономиках, где регуляторные механизмы зачастую не успевают за темпами цифровых инноваций. В статье предлагается модель Интегрированной Архитектуры Цифрового Управления (Integrated Digital Governance Architecture – IDGA), которая обеспечивает согласование внедрения финансовых технологий с институциональной безопасностью. Результаты исследования показывают, что эффективное управление выступает не только инструментом обеспечения соответствия требованиям, но и стратегическим фактором формирования долгосрочной цифровой финансовой устойчивости.

Ключевые слова: Цифровые финансовые риски, системы внутреннего контроля, корпоративное управление, развивающиеся экономики, Теория агентских отношений (Agency Theory), Теория динамических способностей (Dynamic Capabilities Theory), организационная устойчивость**.**

Introduction

The rapid digital transformation of financial systems over the last decade has significantly altered the operational environment for both financial entities and non-financial businesses. Advancements such as mobile payment solutions, blockchain transactions, AI-based credit assessments, and cloud-based financial systems have created substantial efficiencies and broadened market opportunities (Gomber et al., 2017). Nevertheless, this shift to digital has introduced new challenges: organizations must now navigate a landscape filled with novel and intricate risk factors that traditional governance models were not equipped to handle.

Digital financial risks, including cybersecurity incidents, algorithmic errors, failures of third-party vendors, and technology-facilitated financial fraud, constitute a distinctly different category of organizational hazards. In contrast to traditional financial risks, these threats can emerge swiftly, spread through interconnected networks, and result in damage that goes beyond just financial loss, affecting reputation and inviting regulatory penalties (Arner et al., 2016). The repercussions of insufficient digital risk governance were starkly highlighted by notable events like the cyber theft at Bangladesh Bank, extensive data breaches at financial institutions, and disruptions in algorithmic trading within equity markets.

Despite an increasing awareness of these risks, a significant disparity remains between the swift uptake of digital financial technologies and the governance frameworks necessary to protect organizational integrity. Governance structures that were originally designed around periodic reporting and human-driven fraud prevention are proving inadequate in scenarios where transactions happen in milliseconds and threats continuously evolve (Tricker, 2019).

This gap is particularly evident in developing economies, where regulatory frameworks frequently lag behind the pace of technological advancement. This paper seeks to bridge this gap through a conceptual-analytical approach by exploring how internal control systems and corporate governance structures can be redefined and enhanced to effectively manage digital financial risks.

Research Objectives

This study is guided by three interconnected research objectives that collectively aim to advance understanding of digital financial risks governance:

1. The first objective is to identify and define the primary categories of digital financial risk that organizations face in the modern digital economy, distinguishing them from conventional financial risks and establishing the basis for tailored governance responses.

2. The second objective is to examine the limitations of existing internal control and corporate governance frameworks in addressing these risks, with particular attention to the structural and temporal gaps that render traditional mechanisms insufficient in digital environments.
3. The third objective is to propose an integrated governance-oriented framework that organizations, and particularly those in developing countries, can adopt as a conceptual reference for strengthening their digital financial risk management capabilities, informed by established theoretical perspectives in management and organizational studies.

Literature Review

The notion of digital financial risk has significantly progressed within academic discourse. Initially, research tended to classify information technology risk as a subset of operational risk, adhering to the categorization established by the Basel II framework (Basel Committee on Banking Supervision, 2006). Nevertheless, contemporary research advocates for recognizing digital financial risk as a separate entity, highlighting its systemic, rapid emergence, and transboundary features (Ruan, 2019).

Researchers have suggested various classifications of these risks. Arner et al. (2026) categorize risks into three types: those stemming from technological infrastructure (such as system failures and cybersecurity breaches), those linked to digital business models (including platform concentration and dependencies on third parties), and those resulting from regulatory deficiencies (such as unregulated fintech operations). For this paper, digital financial risks are defined to include: (1) cybersecurity risk, which encompasses data breaches and ransomware incidents; (2) digital fraud risk, which covers identity theft and payment fraud; (3) algorithmic and model risk that emerges from automated decision-making processes; and (4) third-party and supply chain risk related to reliance on external technological service providers.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework continues to serve as the primary reference for designing internal controls, emphasizing five key components: control environment, risk assessment, control activities, information and communication, and monitoring (COSO, 2013). Critics maintain that this framework is fundamentally designed for periodic and structured review processes, which are not well-suited to the continuous and dynamic nature of digital risk (Vasarhelyi et al., 2015).

Continuous auditing and monitoring (CAM), characterized as the real-time, automated evaluation of financial data and controls, has been identified as an essential innovation in addressing this issue (Vasarhelyi et al., 2015). Research by Huang et al. (2017) indicates that organizations with more technologically advanced internal audit capabilities demonstrate lower rates of material misstatements. The incorporation of artificial intelligence and machine learning into fraud detection systems represents a new frontier, with preliminary findings indicating notable enhancements in detection accuracy compared to rule-based systems (West & Bhattacharya, 2016).

Scholarships in corporate governance has increasingly acknowledged the limitations of traditional board oversight mechanisms within digital contexts. Often, boards of directors lack the technical knowledge required to effectively supervise complex digital risk exposures (Hines & Peters, 2015). Survey data consistently reveal that a significant majority of corporate directors feel inadequately informed about the cybersecurity risks faced by their organizations (National Association of Corporate Directors, 2020).

In response, governance scholars have suggested structural changes, including the establishment of dedicated technology or cybersecurity committees at the board level, the appointment of directors with technological expertise, and the incorporation of chief information security officers (CISOs) into executive reporting lines (Tricker, 2019; Hines & Peters, 2015). In emerging economies, additional obstacles arise due to concentrated ownership structures, weaker institutional investor activism, and less robust regulatory enforcement, all of which can hinder effective governance (Claessens & Yurtoglu, 2013).

Methodology

This study employs a conceptual-analytical research framework, which is suitable for synthesizing established knowledge, applying theoretical perspectives to a less explored issue, and creating a coherent structure for future empirical research (Jaakkola, 2020). In contrast to empirical research designs that depend on the collection of primary data through methods such as surveys, interviews, or experiments, a conceptual approach utilizes existing academic literature and theoretical frameworks to systematically analyze the phenomenon under consideration. This methodology is particularly fitting for the current research question for two key reasons. Firstly, the governance of digital financial risks represents a rapidly changing field where empirical data is frequently proprietary, fragmented geographically, or lacks sufficient longitudinal depth to enable strong statistical conclusions. Secondly, the main contribution of this paper, a synthesized governance framework, is fundamentally conceptual, necessitating theoretical foundations rather than empirical measurement. Consequently, this paper adheres to the methodological tradition of conceptual contributions in management and governance research, similar to seminal works on Agency Theory and organizational capabilities (Jensen & Meckling, 1976; Teece et al., 1997).

Two theoretical frameworks are utilized as the primary analytical lenses for examining the governance of digital financial risks. These frameworks were chosen because they tackle complementary aspects of the governance challenge: incentive alignment and information asymmetry on one side, and organizational adaptability on the other. The first analytical lens is Agency Theory, originally developed by Jensen and Meckling (1976) and expanded upon by Eisenhardt (1989). Agency Theory elucidates how the relationships between principals (like shareholders and regulators) and agents (such as managers and technology providers) are influenced by information asymmetries and conflicting incentives. This framework is particularly effective in diagnosing the reasons for the inadequacy of existing governance mechanisms in digital contexts, where technical complexities significantly increase the informational divide between principals and agents. The second analytical lens is Dynamic Capabilities Theory, introduced by Teece et al. (1997) and further refined by Teece (2007). This framework views organizational performance in volatile environments as a function of the firm's capacity to recognize changes, capitalize on opportunities, and reconfigure resources. When applied to the governance of digital risks, Dynamic Capabilities Theory offers terminology for articulating what adaptive governance entails in practice, which is shifting the analytical emphasis from static compliance controls to ongoing organizational learning and responsiveness.

The analysis unfolds in two phases. In the initial phase, the two theoretical lenses are applied to the governance challenges identified in the literature, yielding theoretically grounded insights regarding the specific mechanisms by which current frameworks are inadequate. In the subsequent phase, these insights are amalgamated into a proposed governance framework, the Integrated Digital Governance Architecture (IDGA), which consists of three pillars that reflect the complementary prescriptive implications of the two theories. This methodology ensures that the framework is not merely descriptive but is logically constructed based on established theoretical tenets.

Results and Analysis

Finding 1: The Temporal Mismatch Between Digital Risk and Governance Cycles

The initial observation from utilizing theoretical frameworks on the literature indicates a significant temporal discrepancy between the pace at which digital financial risks emerge and the rhythm of conventional governance practices. Traditional governance functions on quarterly reporting intervals, annual audits, and regular board assessments, or timelines that are fundamentally incompatible with the rapidity of digital risk. A sophisticated cyber intrusion can compromise sensitive information within hours, while algorithmic trading errors can lead to substantial financial losses in mere minutes (Kirilenko et al., 2017). From the perspective of Agency Theory, this temporal mismatch is not just a logical issue; it constitutes a governance failure that exacerbates information asymmetry. By the time traditional oversight identifies a problem, agents may have already hidden its source, resulting in potentially irreversible reputational or financial harm. Dynamic Capabilities Theory supports this assessment: organizations that cannot sense changes in real time are unable to respond effectively or adapt quickly. The analytical conclusion is that governance structures need to

evolve from intermittent to continuous monitoring systems. Continuous control monitoring (CCM) systems, which employ automated data analytics to evaluate financial transactions and system operations in real time, effectively bridge this gap. Organizations that have adopted CCM platforms report significant enhancements in fraud detection rates and markedly reduced timeframes between the occurrence of incidents and their detection (Vasarhelyi et al., 2015). This finding directly pertains to Research Objective 2.

Finding 2: Board Competency Deficits and Structures Governance Gaps

The second discovery relates to the inherent inadequacy of board-level governance in environments characterized by digital risk. The literature consistently indicates that boards of directors, usually comprised of individuals with expertise in finance, law, and general management, often lack the necessary technical knowledge to manage digital risk exposures effectively (Hines & Peters, 2015). This signifies a qualitative decline in governance efficacy as digital risks become increasingly complex. Agency Theory clearly highlights this shortcoming: when principals (boards) are unable to accurately interpret the information provided by their agents (CISOs, IT managers, algorithmic system operators), the monitoring function of governance deteriorates, irrespective of its formal structure. Boards receive cybersecurity reports they cannot analyze, approve technology investments they cannot evaluate, and supervise digital transformation strategies whose risk implications they fail to fully understand. The structural changes suggested by both theories include establishing dedicated technology or cybersecurity committees at the board level with the necessary expertise; ensuring direct reporting lines from the chief information security officer to the board, bypassing middle management; integrating digital risk considerations into the formal charters of audit committees; and implementing ongoing digital risk literacy programs for the board. These modifications restore the informational conditions required for effective oversight by principals and enhance the board's sensing capabilities as proposed by Dynamic Capabilities Theory.

Finding 3: Compounded Vulnerabilities in Emerging Economies

The third discovery focuses on the unique governance obstacles encountered by organizations in emerging markets, an aspect that directly relates to Research Objectives 1 and 2. In these environments, the speed of adopting digital financial solutions has significantly surpassed the development of adequate governance skills and regulatory structures. While mobile financial services, digital payment systems, and FinTech applications have expanded quickly, the regulatory frameworks often remain disjointed and are typically designed around conventional financial products (Claessens & Yurtoglu, 2013). The concentration of ownership, a characteristic of many corporate settings in emerging markets, adds further complexity. Dominant shareholders may exert influence over board composition and internal audit processes in ways that compromise the independence required for effective oversight of digital risks. From the perspective of Agency Theory, concentrated ownership leads to agency conflicts between controlling and minority shareholders, layering these issues on top of the traditional manager-shareholder conflict, thereby creating multifaceted governance challenges that standard frameworks fail to address adequately. Simultaneously, Dynamic Capabilities Theory presents a significant opportunity: the lack of entrenched legacy governance systems in many organizations within emerging markets can enable a quicker adoption of contemporary, technology-focused governance tools. Instead of adapting digital capabilities to outdated institutional structures, organizations in these settings can potentially create flexible governance systems from scratch, a form of institutional leapfrogging similar to the mobile banking revolution that bypassed traditional bank branches in various African and Asian regions.

Proposed Framework: Integrated Digital Governance Architecture (IDGA)

Drawing from the three findings outlined and integrating the prescriptive implications of both theoretical frameworks, this paper introduces the Integrated Digital Governance Architecture (IDGA) as a response to Research Objective 3. The IDGA consists of three interrelated pillars, each addressing a specific aspect of the governance challenge identified in the analysis.

Pillar I – Continuous Intelligence Infrastructure – tackles the temporal mismatch issue (Finding 1) by establishing real-time monitoring as the operational base for digital risk governance. This

includes continuous control monitoring platforms, automated anomaly detection systems, threat intelligence feeds, and the incorporation of data literacy across all governance levels. By offering principals continuous, technology-facilitated visibility into system behavior, this pillar directly mitigates the information asymmetry highlighted by Agency Theory and enhances the sensing capability advocated by Dynamic Capabilities Theory.

Pillar II – Adaptive Governance Structures – responds to the board competency and structural weaknesses identified in Finding 2. It involves the establishment of dedicated technology and cybersecurity board committees, direct reporting lines for Chief Information Security Officers (CISOs), the integration of digital risk into audit committee charters, and board-level digital literacy initiatives. These structural changes restore effective oversight conditions for principals and equip governance bodies with the necessary decision-making frameworks to address digital risks as they arise promptly.

Pillar III – Regulatory Alignment and Ecosystem Integration – tackles the challenges posed by the institutional environment as highlighted in Finding 3, particularly pertinent to emerging economies. This includes engagement in regulatory standard-setting processes, adoption of globally recognized control frameworks (such as ISO 27001 and the NIST Cybersecurity Framework, as well as updated COSO guidance), participation in industry information-sharing platforms, and robust third-party risk management protocols. This pillar represents the reconfiguring capability described in Dynamic Capabilities Theory, allowing the organizations to learn from the wider ecosystem and systematically adapt their governance frameworks in response to changing regulatory and threat environments.

Discussion

The results and suggested framework have significant implications for both academic research and organizational practices. From a theoretical perspective, this pillar illustrates how Agency Theory and Dynamic Capabilities Theory, frameworks that were originally conceived in non-digital settings, can be effectively adapted to address modern governance issues. The combination of these two approaches represents a valuable contribution: Agency Theory identifies the informational and incentive challenges that complicate digital governance, while Dynamic Capabilities Theory suggests the necessary adaptive organizational strategies for achieving digital resilience. Utilizing either framework in isolation is inadequate.

On a practical level, the IDGA framework provides organizations with a systematic approach for self-assessing their governance. By measuring their existing capabilities against the three pillars of the framework, organizations can pinpoint key areas needing investment and improvement. Crucially, the framework avoids the reductionist view of digital governance as merely a technological issue. Although Pillar I relies on technology, Pillars II and III highlight the importance of institutional design, human skills, and relational engagement as equally vital factors in fostering digital resilience, a balance that is often overlooked in practitioner-focused cybersecurity frameworks.

For policymakers in developing nations, the framework indicates that regulatory initiatives should emphasize proportionality and flexibility, creating regulations that can adapt alongside the technologies they are meant to oversee, rather than striving to regulate a static technological environment comprehensively. International collaboration and capacity-building efforts can expedite this process by facilitating the exchange of regulatory knowledge and supervisory skills.

Several limitations must be recognized. The paper does not provide empirical evidence to validate the effectiveness of the IDGA framework; this remains a crucial area for future quantitative and qualitative research, ideally through multi-country case studies or survey-based evaluations of the framework's assertions. The framework is inherently broad in its design and will necessitate adaptation to specific contexts to reflect industry specifics, organizational size, and regulatory circumstances. Lastly, the swiftly changing nature of digital financial technologies implies that even the most well-founded governance frameworks should be regarded as dynamic entities, a concept that is fundamentally integrated within the Dynamic Capabilities pillar itself.

Conclusion

This paper has explored the essential role of internal controls and corporate governance frameworks in managing digital financial risks. Using a conceptual-analytical approach based on Agency Theory and Dynamic Capabilities, it uncovered three primary governance challenges: a temporal discord between the rapid pace of digital risks and governance cycles; deficiencies in board-level competencies and structural inadequacies; and heightened institutional vulnerabilities in emerging markets. In light of these insights, the paper introduced the Integrated Digital Governance Architecture (IDGA). This three-tiered framework includes continuous intelligence infrastructure, adaptive governance structures, and the alignment of regulations with ecosystem integration.

The paper successfully addressed its three research objectives. The first objective, which aimed to characterize digital financial risk, was achieved through the taxonomy established in the literature review and further refined in the analysis. The second objective, concerning the examination of the limitations of current frameworks, was tackled through findings grounded in theory regarding temporal mismatches and competency deficiencies at the board level. The third objective, which involved proposing an integrated framework, was accomplished with the IDGA, whose components logically arise from the analytical findings.

In conclusion, this paper contends that effective governance of digital risks should not be viewed as a mere compliance obligation but rather as a strategic necessity. Organizations that invest in governance architectures capable of addressing digital financial risks are more likely not only to avert severe losses but also to foster the institutional trust essential for sustainable engagement in the digital economy. As the pace of financial digitalization accelerates worldwide, the governance frameworks established today will shape organizational resilience and credibility for the future.

References

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of Fintech: A new post-crisis paradigm? *Georgetown Journal of International Law, 47*(4), 1271-1319.
2. Basel Committee on Banking Supervision. (2006). *International convergence of capital measurement and capital standards: A revised framework*. Bank for International Settlements.
3. Claessens, S., & Yurtoglu, B. B. (2013). Corporate governance in emerging markets: A survey. *Emerging Markets Review*, 15, 1-33. (Available at: https://doi.org/10.1016/j.ememar.2012.03.002)
4. Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal Control – Integrated framework*. AICPA.
5. Eisenhardt, K. M. (1989). Agency Theory: An assessment and review. *Academy of Management Review*, 14(1), 57-74. (Available at: https://doi.org/10.5465/amr.1989.4279003)
6. Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537-580. (Available at: https://doi.org/10.1007/s11573-017-0852-x)
7. Hines, C. S., & Peters, G. F. (2015). Voluntary board adoption of a standing cybersecurity committee: Determinants and consequences. *Managerial Auditing Journal, 30*(8/9), 861-893.
8. Huang, S.-Y., Tsaih, R.-H., & Lin, W.-Y. (2017). Unsupervised neural networks approach for understanding fraudulent financial reporting. *Industrial Management & Data Systems, 117*(2), 342-359.
9. Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review, 10*, 18–26. (Available at: https://doi.org/10.1007/s13162-020-00161-0)
10. Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360. (Available at: https://doi.org/10.1016/0304-405X(76)90026-X)
11. Kirilenko, A., Kyle, A. S., Samadi, M., & Tuzun, T. (2017). The flash crash: High-frequency trading in an electronic market. *Journal of Finance, 72*(3), 967-998. (Available at: https://doi.org/10.1111/jofi.12498)
12. National Association of Corporate Directors (NACD). (2020). *2019-2020 NACD public company governance survey.* NACD.

13. Ruan, K. (2019). Defining and classifying cyber risk for financial stability. *Geneva Papers on Risk and Insurance — Issues and Practice, 44*(2), 338-354.
14. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319-1350. (Available at: https://doi.org/10.1002/smj.640)
15. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal, 18*(7), 509-533.
16. Tricker, R. I. (2019). *Corporate governance: Principles, policies, and practices* (4th ed.). Oxford University Press.
17. Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & Littley, J. (2015). The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems, 13*(3), 267-281.
18. West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47-66. (Available at: https://doi.org/10.1016/j.cose.2015.09.005)