American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Internal Control Adaptation for Platform-Based Business Models

Dr. James Whitaker

Professor, University of Manchester, United Kingdom

Abstract

Platform-based business models have altered the organizational boundaries within which internal control systems traditionally operate. Unlike conventional firms, platform enterprises coordinate transactions, information, payments, algorithms, application programming interfaces, complementors, service providers, and users across digitally interconnected ecosystems. This structure creates control challenges that cannot be adequately addressed through static authorization procedures, periodic reconciliations, or controls designed primarily around internally owned processes. The present study develops a conceptual–methodological framework for adapting internal controls to platform-based business models. It integrates established internal-control principles with research on digital platforms, ecosystem governance, boundary resources, and technology-enabled monitoring. The study applies a structured conceptual synthesis and scenario-based analytical model rather than claiming observations from an actual organizational sample. Five major control domains are examined: ecosystem participant governance, digital transaction integrity, algorithmic accountability, data and access governance, and continuous monitoring.

A simulated maturity analysis illustrates how conventional control effectiveness may decline as platform complexity increases, whereas adaptive controls designed around real-time monitoring, distributed accountability, configurable access, and ecosystem-level risk identification can retain stronger control effectiveness. The paper argues that platform organizations require a transition from organization-centric internal control toward ecosystem-aware control architecture. Effective adaptation does not imply replacing established internal-control frameworks; rather, it requires translating their principles into controls capable of functioning across dynamic technological boundaries and partially autonomous actors. The proposed framework contributes to the literature by linking platform governance and internal control and provides a practical basis for managers, auditors, controllers, and governance bodies seeking to strengthen accountability without unnecessarily constraining platform innovation.

Keywords: internal control, platform-based business model, digital platform governance, ecosystem risk, continuous monitoring, algorithmic accountability, digital transactions, control adaptation

1. Introduction

Platform-based business models have become an important organizational form in digital commerce, financial services, transportation, professional services, software, retail, media, and numerous other

sectors. Rather than producing value exclusively through internally controlled assets and linear value chains, platform organizations frequently enable interactions among multiple groups of participants. Their operations may depend on external sellers, developers, service providers, payment intermediaries, logistics partners, cloud providers, advertisers, and end users. Research on digital platforms consequently emphasizes their programmable, extensible, and ecosystem-oriented characteristics. De Reuver, Sørensen, and Basole describe digital platforms as an increasingly important research domain in which technological architecture, market relationships, and organizational arrangements interact dynamically. These characteristics fundamentally change the location and nature of organizational control.

Traditional internal-control systems were generally developed around identifiable organizational processes, relatively stable reporting relationships, defined responsibilities, and transactions occurring within controlled information systems. The COSO Internal Control—Integrated Framework remains a widely recognized principles-based foundation for supporting operational, reporting, and compliance objectives and was refreshed in 2013. Its principles remain relevant to digital organizations; however, the operational mechanisms through which those principles are implemented must evolve when transactions are executed through APIs, automated rules, third-party interfaces, cloud services, and algorithmic decision systems. The challenge is therefore not the abandonment of conventional internal-control theory but its translation into a substantially different operating environment.

Platform organizations also differ from conventional firms because important resources and decisions may be distributed among actors that are economically connected but organizationally independent. Jacobides, Cennamo, and Gawer explain that ecosystems depend on relationships among actors whose activities are complementary yet not governed solely through conventional hierarchical authority. Wareham, Fox, and Cano Giner similarly identify governance tensions involving control and autonomy, standardization and variety, and collective versus individual interests in technology ecosystems. These tensions are directly relevant to internal control because excessive restrictions may weaken innovation and participation, while insufficient control can increase exposure to fraud, unauthorized access, inaccurate reporting, manipulation, regulatory violations, or failures by ecosystem participants.

A further difficulty arises from the speed and volume of platform transactions. High-frequency digital interactions can make periodic control testing inadequate for risks that materialize within seconds or minutes. Digital control environments therefore increasingly require automated validation, exception detection, identity and access controls, audit trails, continuous reconciliation, configurable risk thresholds, and monitoring of technological dependencies. Industry guidance on digital control transformation has similarly recognized that digital technologies affect control procedures, risk management, monitoring, and audit activities. The effectiveness of an internal-control system in a platform organization must consequently be evaluated not only by whether controls formally exist but also by whether those controls remain responsive as the platform changes.

Against this background, the present study examines how internal-control architecture can be adapted for platform-based business models while preserving accountability, reliability, and risk responsiveness. The paper develops a structured framework linking conventional internal-control principles with ecosystem governance, digital boundary management, automated monitoring, and

algorithmic accountability. Because no primary organizational dataset has been supplied, the analysis is explicitly conceptual and simulation-based. It does not represent simulated values as observed corporate results. The intended contribution is a theoretically grounded model that can subsequently be tested through surveys, case studies, audit evidence, longitudinal platform data, or comparative organizational research.

2. Objectives of the Study

2.1 Conceptual Objective: Reframing Internal Control Around Platform Architecture

The first objective is to determine how the meaning of an effective control environment changes when organizational value creation depends substantially on platform architecture and ecosystem participation. Traditional controls usually identify process owners, transaction initiators, approvers, record keepers, and reviewers inside a clearly defined organization. Platform activities may instead involve sequences in which several independent parties contribute data or decisions before a transaction is completed. Internal control must therefore identify not only organizational responsibilities but also control responsibilities attached to digital interfaces, partner relationships, automated rules, and ecosystem access rights.

The study consequently seeks to connect platform architecture with control architecture. This connection requires analysis of where economic events originate, how information moves through platform layers, which actors can modify it, and where evidence of authorization or validation is recorded. The conceptual objective is not to create separate control principles for digital platforms but to establish how established principles can be operationalized when organizational boundaries are porous and technology mediates most transactions.

2.2 Analytical Objective: Identifying Priority Domains for Adaptive Control

The second objective is to identify the areas in which platform complexity creates the greatest need for control adaptation. Five domains are emphasized: ecosystem participant governance, transaction integrity, algorithmic accountability, data and access governance, and continuous monitoring. These domains were selected because they capture both traditional control concerns and risks produced by platform interdependence.

The analysis also examines the proposition that control effectiveness depends increasingly on adaptability as a platform matures. A static system may appear adequate during an early platform stage when transaction volumes, partner numbers, and technological integrations remain limited. As APIs proliferate, complementors increase, automated decision rules become more influential, and multiple participant groups interact simultaneously, the same controls may become less effective. The study therefore evaluates adaptive control as a capability rather than a one-time compliance configuration.

3. Review of Literature

3.1 Platform Architecture, Ecosystems, and Distributed Governance

Early platform research recognized that software-based platforms create ecosystems in which architectural design and governance mechanisms evolve together. Tiwana, Konsynski, and Bush argue that platform evolution reflects the interaction of architecture, governance, and environmental dynamics. This perspective is important for internal control because risk does not remain constant when a platform

changes its technical interfaces, participation rules, or ecosystem boundaries. A control that is suitable when all services are developed internally may become insufficient when functionality is opened to third-party developers or external service providers.

Gawer and Cusumano distinguish company-specific platforms from broader industry platforms and emphasize the importance of technological design, organizational choices, intellectual-property arrangements, and external relationships in ecosystem innovation. From an internal-control perspective, these design decisions alter who can initiate transactions, obtain information, introduce software components, and influence customer outcomes. Platform governance is therefore inseparable from risk governance. A platform rule determining who may enter an ecosystem, for example, can simultaneously operate as a strategic governance mechanism and a preventive internal control.

Eaton, Elaluf-Calderwood, Sørensen, and Yoo demonstrate through the Apple iOS service-system context that boundary resources are not necessarily static; they can be continually reshaped through interactions among heterogeneous actors and technologies. This observation has significant control implications. APIs, software development kits, technical permissions, identity mechanisms, data interfaces, and platform policies are not merely technological resources. They also determine the boundary through which participants interact with the platform and can therefore serve as embedded control mechanisms.

3.2 Internal-Control Principles in Digitally Mediated Operations

The COSO framework provides a principles-based structure organized around the control environment, risk assessment, control activities, information and communication, and monitoring. Its continued relevance to technology-intensive environments lies in the flexibility of these principles rather than in any fixed catalogue of manual procedures. In platform organizations, the control environment must encompass digital accountability, the risk-assessment process must include ecosystem and technology dependencies, control activities must increasingly be automated, information flows must be traceable across interfaces, and monitoring should operate at a frequency appropriate to digital transaction speed.

The literature on ecosystem governance strengthens this interpretation. Wareham, Fox, and Cano Giner demonstrate that governance mechanisms must balance competing ecosystem tensions rather than seek absolute centralized control. Constantinides, Henfridsson, and Parker further show that digital platforms and infrastructures create distinctive organizational and technological relationships. Internal controls in these environments must therefore be calibrated. The objective is not to eliminate participant autonomy but to define minimum standards, verification points, access restrictions, escalation rules, and accountability structures that keep distributed participation within the organization's risk tolerance.

Digital transformation also changes the evidence available for control evaluation. Automated workflows can generate granular logs, time stamps, authentication records, transaction histories, configuration records, and machine-generated exceptions. When properly governed, this information can strengthen monitoring by shifting assurance from retrospective sampling toward more continuous observation. At the same time, automation can concentrate risk when a defective rule is applied to thousands of transactions. Platform internal control consequently requires both automated execution and independent validation of the logic governing that automation.

3.3 Research Gap: From Enterprise Controls to Ecosystem-Aware Controls

Platform-management literature has developed sophisticated explanations of architecture, complementarity, ecosystem participation, innovation, and governance. De Reuver, Sørensen, and Basole specifically emphasize the growing complexity and broad industry relevance of digital-platform research. Internal-control research and professional frameworks, in contrast, have traditionally been applied at organizational and process levels. Although the underlying principles remain applicable, there is comparatively less integration between platform-governance theory and the practical design of internal-control systems.

This creates an important conceptual gap. Platform governance frequently examines who may participate, what actors may develop, which resources are accessible, and how ecosystem relationships are coordinated. Internal control examines whether organizational objectives are achieved with acceptable exposure to operational, reporting, and compliance risk. These concerns overlap extensively, yet they are often discussed separately. Participant admission rules, API permissions, seller verification, algorithm-change approvals, digital audit trails, automated reconciliations, and exception-management rules can simultaneously function as governance mechanisms and internal controls.

The present study addresses this gap through an ecosystem-aware control model. It proposes that internal-control design should follow the actual path of platform value creation rather than organizational boundaries alone. Consequently, controls should be mapped to interactions among actors, data, algorithms, payments, digital identities, and technological interfaces. This approach preserves established control principles while making their application responsive to the structural characteristics of platform business models.

4. Research Methodology

4.1 Research Design and Conceptual Synthesis

The study adopts a conceptual–methodological research design. It does not claim to report primary survey responses, interviews, archival financial data, or operational records from an actual company. Instead, the study synthesizes established internal-control concepts with peer-reviewed platform and ecosystem-governance literature. This design is suitable for developing a theoretically coherent framework before its subsequent empirical validation.

The analytical unit is the platform control domain, defined as an area in which platform architecture, participant behavior, technological configuration, or digital information flows create a material requirement for control. The analysis begins with traditional internal-control objectives and then identifies how the underlying control mechanisms must change when a business moves from relatively closed operations toward multi-actor platform coordination.

4.2 Control-Domain Coding and Assessment Logic

Five control domains were developed from recurring concerns identified across the internal-control and platform-governance literature. Each domain was examined through four dimensions: principal risk, conventional control response, limitation of the conventional response, and adaptive control requirement. This structure makes the analytical process transparent and suitable for replication in future empirical studies.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 1: Analytical Coding Framework for Platform Internal Control

Control Domain	Principal Platform Risk	Conventional Control Orientation	Adaptive Control Requirement
Ecosystem participant governance	Misconduct or failure by external participants	Contract approval and periodic review	Risk-tiered onboarding, continuous participant monitoring, dynamic permissions
Digital transaction integrity	High-volume erroneous or manipulated transactions	Reconciliation and supervisory review	Automated validation, exception analytics, real-time reconciliation
Algorithmic accountability	Undetected error or bias in automated rules	General IT change approval	Model ownership, version control, validation, outcome monitoring
Data and access governance	Unauthorized access or inappropriate data use	User-access lists and periodic certification	Identity-based controls, least privilege, API authorization, behavioral monitoring
Continuous monitoring	Delayed detection of control failure	Periodic internal-control testing	Continuous indicators, automated alerts, threshold-based escalation

The framework treats adaptation as a change in control design produced by changes in platform complexity. The underlying control objective remains stable—for example, preventing unauthorized activity—while the control mechanism becomes more technologically embedded, data-driven, and responsive. This distinction is important because adaptation should not be confused with uncontrolled procedural change.

4.3 Scenario-Based Simulation Procedure

To illustrate the conceptual relationship between platform maturity and control effectiveness, a simple scenario-based simulation was constructed. Four maturity stages were used: launch, scaling, ecosystem expansion, and multi-sided maturity. Two hypothetical control configurations were compared. The first represents a predominantly static design based on periodic review and controls established at an earlier organizational stage. The second represents an adaptive design incorporating automated monitoring, dynamic access governance, partner-risk reassessment, algorithm-change controls, and continuous exception analysis.

A Simulated Control Effectiveness Index (SCEI) was used only for analytical illustration:

[SCEI=\frac{\sum_{i=1}^{n} w_i c_i}{\sum_{i=1}^{n} w_i}\times100]

where (c_i) represents the simulated effectiveness score assigned to control domain (i), and (w_i) represents its analytical risk weight. The resulting scores are not empirical estimates and should not be

interpreted as measured percentages for real firms. Their purpose is to show the predicted directional effect of failing to redesign controls while platform complexity increases.

5. Analysis

5.1 Platform Complexity and the Declining Fit of Static Controls

The analytical model suggests that static controls experience a progressive loss of fit as platform complexity increases. At the launch stage, organizational leaders may directly supervise major decisions, participant numbers may be small, and most integrations may remain under close technical control. Under these circumstances, conventional approval and review mechanisms can still capture a considerable proportion of relevant risks. Their limitations become more visible during rapid scaling.

As the platform expands, transaction volume can increase faster than manual review capacity. External participants create additional information and conduct risk, APIs multiply the number of technical entry points, and automated decisions become more consequential. A periodic control may therefore continue to operate exactly as designed while becoming less capable of addressing the actual risk. This distinction between control operation and control relevance is central to the proposed framework.

5.2 Comparative Scenario Analysis

The simulated results illustrate the expected difference between static and adaptive control systems. The adaptive configuration does not begin dramatically above the static configuration because sophisticated automation is not necessarily critical at low complexity. Its advantage becomes more substantial as the platform becomes increasingly interconnected.

Table 2: Simulated Control Effectiveness Across Platform Maturity Stages

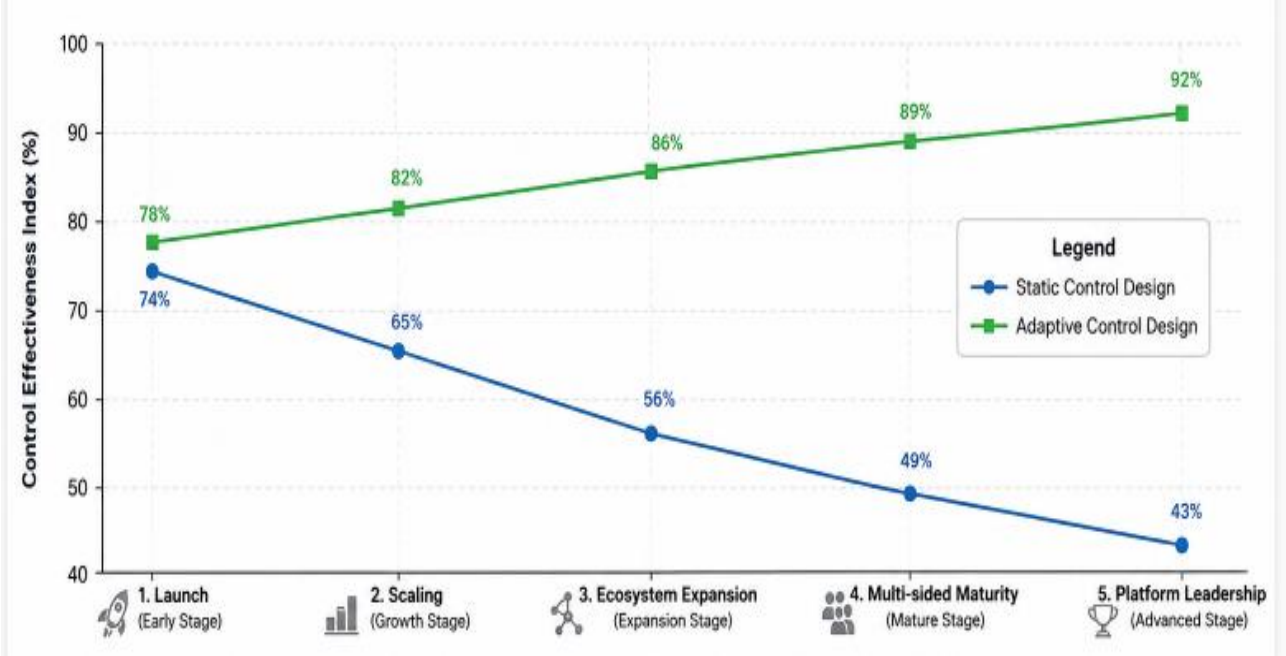
Platform Maturity Stage	Static Control Design (%)	Adaptive Control Design (%)	Effectiveness Gap
Launch	74	78	+4
Scaling	65	82	+17
Ecosystem expansion	56	86	+30
Multi-sided maturity	49	89	+40

Note: Values are hypothetical scenario scores developed exclusively for conceptual analysis. They are not observations from a company, survey, experiment, or secondary dataset.

The simulated effectiveness gap rises from four percentage points during launch to forty percentage points at multi-sided maturity. This pattern reflects the conceptual proposition that control adaptability becomes increasingly valuable as platform activity moves beyond direct organizational

supervision. Static controls deteriorate not necessarily because they are poorly executed but because the operating model has outgrown the assumptions under which they were designed.

Graph 1: Control Effectiveness as Platform Complexity Increases



The graph demonstrates an important theoretical relationship. Increasing digital complexity does not automatically weaken internal control. Weakening occurs when control architecture remains unchanged while the business architecture becomes more distributed. An adaptive system can instead use greater digitalization to strengthen traceability, automate verification, identify exceptions, and monitor risk indicators at a speed that would be impractical through manual procedures.

5.3 Adaptive Control Architecture for Platform Organizations

The analysis supports a layered adaptive-control architecture. The first layer is participant control, covering identity verification, onboarding, contractual obligations, risk classification, conduct monitoring, and suspension rights. Platform organizations must know not simply who their contractual counterparties are but also which digital privileges those counterparties possess and whether their behavior remains consistent with established rules.

The second layer concerns transaction and technology controls. These include API authentication, automated transaction validation, integrity checks, reconciliation, system logging, configuration management, segregation of digital privileges, and controlled deployment of software or algorithmic changes. The control objective should be embedded as closely as possible to the point at which a transaction or technological event occurs.

The third layer is adaptive monitoring and governance. Board-level and managerial oversight should receive information on control exceptions, participant-risk movements, major algorithmic changes, access anomalies, unresolved incidents, data-integrity failures, and recurring control overrides. Monitoring thus becomes an organizational learning mechanism. Control deficiencies are not treated

only as isolated incidents; they provide evidence that risk thresholds, platform rules, technical controls, or governance structures may require recalibration.

6. Discussion

6.1 Internal Control as an Ecosystem Governance Capability

The findings suggest that internal control in platform businesses should be understood as an ecosystem governance capability rather than a narrowly administrative function. Jacobides, Cennamo, and Gawer's ecosystem perspective emphasizes interdependence among autonomous yet complementary actors. This structure makes hierarchical supervision insufficient as the sole form of control. Platform firms must govern behavior through access conditions, standards, interfaces, incentives, monitoring, contractual mechanisms, and technological restrictions.

This interpretation also explains why platform governance and internal control frequently overlap. A requirement that sellers verify their identities, for example, may protect users while simultaneously reducing fraud exposure. API rate limits may protect technological stability while also reducing unauthorized extraction or manipulation. Developer certification may support ecosystem quality while acting as a preventive control. Effective internal control therefore becomes embedded within platform design rather than added after operations have been constructed.

Such integration can also reduce unnecessary conflict between innovation and control. Platform literature shows that governance must balance control with participant autonomy. Controls that specify acceptable outcomes, access boundaries, evidence requirements, and escalation thresholds may allow more flexibility than controls requiring approval of every activity. Adaptive internal control should therefore be sufficiently strong to protect organizational objectives while remaining proportionate to the risk generated by each participant and activity.

6.2 Continuous Monitoring and Digital Evidence

A second implication concerns the transition from periodic assurance toward continuous or high-frequency monitoring. Platform transactions generate digital evidence at a scale unavailable in many traditional environments. Authentication events, changes in permissions, API requests, transaction timestamps, payment states, error logs, user complaints, configuration changes, and algorithm versions can all support a richer control environment when the information is reliable and appropriately governed.

However, more data do not automatically produce stronger control. Monitoring systems require clearly defined risk indicators, thresholds, responsibility for investigating exceptions, escalation criteria, and evidence that alerts were appropriately resolved. An organization can generate thousands of automated alerts while remaining poorly controlled if warnings are ignored or if thresholds are not calibrated. Adaptive control therefore requires governance of the monitoring mechanism itself.

The strongest platform controls are consequently likely to combine automated detection with accountable human judgment. Automation can identify unusual patterns rapidly, while trained personnel evaluate context, materiality, legitimacy, and required response. This hybrid arrangement avoids the weaknesses of purely manual oversight without assuming that automated rules are inherently reliable.

6.3 Algorithmic Accountability and Control Ownership

Algorithmic decision-making creates an additional control-ownership problem. Conventional process controls usually assign responsibility to identifiable employees or departments. A platform algorithm may affect pricing, ranking, fraud detection, participant suspension, credit allocation, recommendations, advertising placement, or transaction routing. Responsibility must therefore extend beyond the technical team that writes software.

An adaptive control framework should require named ownership of material algorithms, formal change authorization, documented objectives, controlled testing, version records, monitoring of outputs, and procedures for investigating unintended outcomes. These requirements are conceptually consistent with COSO's principles-based orientation because they translate accountability, risk assessment, control activity, information, and monitoring into an algorithm-mediated operating environment.

Algorithmic accountability also strengthens auditability. If an organization cannot determine which model or rule produced a material decision, when that version became active, who approved it, and what data were used, subsequent control evaluation becomes difficult. Internal control adaptation should therefore preserve an evidentiary chain connecting automated outcomes to authorized rules and accountable decision owners.

7. Conclusion

Platform-based business models require a significant reconsideration of how internal controls are operationalized. Their multi-sided structure, dependence on external participants, programmable interfaces, automated decisions, and rapidly changing technological architecture create risks that are difficult to manage through static controls designed primarily for internally bounded processes. The central conclusion of this study is that the principles of internal control remain applicable, but the mechanisms through which those principles are achieved must evolve with the business model.

The proposed framework identifies ecosystem participant governance, transaction integrity, algorithmic accountability, data and access governance, and continuous monitoring as central domains of platform control adaptation. Within these domains, controls should become increasingly embedded, automated, risk-sensitive, and evidence-generating. Platform organizations should therefore evaluate control relevance whenever they change participant rules, open new APIs, introduce new automated decision systems, expand into additional markets, or increase reliance on external service providers.

The scenario analysis reinforces this argument by illustrating that static controls can progressively lose effectiveness as platform complexity grows, whereas adaptive control systems can maintain stronger alignment with the changing risk environment. These results remain conceptual rather than empirical and should be interpreted accordingly. Future research can validate the framework through comparative case studies, questionnaires involving internal auditors and platform managers, archival control-deficiency data, longitudinal studies of platform growth, or field experiments evaluating continuous-monitoring mechanisms.

The study ultimately positions internal-control adaptation as a strategic governance capability. A platform firm cannot rely exclusively on controls imposed after transactions have occurred; accountability must be integrated into platform architecture, participation rules, digital identities, algorithms, interfaces, and monitoring systems. Organizations that align control architecture with

platform architecture are likely to be better positioned to support reliable reporting, responsible innovation, regulatory accountability, stakeholder confidence, and sustainable ecosystem growth.

References

1. Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Böhm, M., & Krcmar, H. (2020). Digital platform ecosystems. *Electronic Markets, 30*, 87–98.
2. Fenwick, M., McCahery, J. A., & Vermeulen, E. P. M. (2019). The end of 'corporate' governance: Hello 'platform' governance. *European Business Organization Law Review, 20*, 171–199.
3. Mukhopadhyay, S., & Bouwman, H. (2019). Orchestration and governance in digital platform ecosystems: A literature review and trends. *Digital Policy, Regulation and Governance, 21*(4), 329–351.
4. Teh, T.-H. (2022). Platform governance. *American Economic Journal: Microeconomics, 14*(3), 213–254.
5. Tiwana, A. (2014). *Platform Ecosystems: Aligning Architecture, Governance, and Strategy*. Morgan Kaufmann.
6. Tiwana, A. (2015). Evolutionary competition in platform ecosystems. *Information Systems Research, 26*(2), 266–281.
7. Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal, 39*(8), 2255–2276.
8. Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. *Organization Science, 25*(4), 1195–1215.
9. Parker, G. G., Van Alstyne, M. W., & Choudary, S. P. (2016). *Platform Revolution: How Networked Markets Are Transforming the Economy—and How to Make Them Work for You*. W. W. Norton.
10. Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Platforms and infrastructures in the digital age. *Information Systems Research, 29*(2), 381–400.
11. Lawson, B. P., Muriel, L., & Sanders, P. R. (2017). A survey on firms' implementation of COSO's 2013 Internal Control–Integrated Framework. *Research in Accounting Regulation, 29*(1), 30–43.
12. Chang, S.-I., Chang, L.-M., & Liao, J.-C. (2020). Risk factors of enterprise internal control under the Internet of Things governance: A qualitative research approach. *Information & Management, 57*(6), 103335.
13. Harrast, S. A. (2020). Robotic process automation in accounting systems. *Journal of Corporate Accounting & Finance, 31*(4), 209–213.
14. Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems, 31*(3), 5–21.
15. Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting, 14*(1), 115–122.
16. Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. *International Journal of Digital Accounting Research, 19*, 21–35.
17. Mo, H. (2023). The impact of digital transformation on internal control quality: A study based on five components of internal control. *Accounting and Corporate Management, 5*, 28–34.

18. Li, X., Zhao, F., & Zhao, Z. (2024). Corporate digital transformation, internal control and total factor productivity. *PLOS ONE*, *19*(3), e0298633.
19. Zhao, T., Yan, N., & Ji, L. (2023). Digital transformation, life cycle and internal control effectiveness: Evidence from China. *Finance Research Letters, 58*, 104223.
20. Chen, Y., & Srinivasan, A. (2023). Digital transformation and internal control quality: Evidence from enterprise information systems. *Journal of Global Information Management*, *31*(6).