STRATEGIC MANAGEMENT OF THE INTERNAL AUDIT FUNCTION IN THE TRANSITION TO A REAL-TIME MODE

Nabeel Ehsan

Integrating Data Governance, Cybersecurity Controls, and Continuous Assurance Frameworks, Dubai, UAE

ABSTRACT

Internal audit of digitally integrated business processes, transactional data flows, and related control environments is undergoing transformation from periodic review toward near real time assurance. Drawing on Agency Theory and Institutional Theory, the study is oriented toward managerial practice and is based on theoretical generalization and analytical interpretation of contemporary approaches to continuous auditing under accelerating digital business processes. The research addresses the critical intersection of data governance, information security, and assurance frameworks essential for organizations operating in digitally interconnected environments. The limitations of the traditional internal audit model based on periodic reviews and sample based testing are examined, and the need to move toward a more dynamic form of assurance that enables timely risk identification is substantiated. Central attention is given to the managerial dimension of internal audit transformation, including changes in the role of the function, revisions of the organizational model, data and technology governance frameworks, competency requirements, and safeguards for preserving independence. The study demonstrates that the practical effectiveness of near real time auditing is determined not by the level of analytical tool adoption, but by their integration into a reproducible control loop with formalized response and escalation conditions. From an operational perspective, such a control loop requires the integration of enterprise data infrastructures with automated monitoring mechanisms. In practice, this involves the use of enterprise resource planning (ERP) systems, security monitoring platforms, and data governance procedures that enable near real time access to transactional information while maintaining strict access controls. The effectiveness of this architecture depends on the coordination between internal audit, information security teams, and data governance structures. Particular emphasis is placed on the cybersecurity and data integrity prerequisites that must be established before continuous monitoring capabilities can be safely deployed. Managerial effects of the transformation related to expanded audit coverage and increased relevance of audit findings are analyzed. Institutional constraints on scaling are also considered, arising from requirements for data controllability and the preservation of the independent status of the internal audit function.

KEYWORDS

internal audit, continuous auditing, strategic management, organizational model, audit independence.

1. INTRODUCTION

1.1. Background and Context

Accelerated digital business processes, increased automation, and the growth of transactional data volumes have substantially altered the temporal dynamics of risks and managerial decisions. In many organizations, events affecting reporting, process stability, and compliance form in a near real time mode, while traditional internal audit remains oriented toward periodic reviews and

sample based testing [7]. Consequently, audit conclusions are often formed with a delay and lose part of their managerial value.

In this study, the term “near real time” refers to audit monitoring performed with minimal operational delay through high frequency data access and automated control procedures, rather than fully instantaneous processing.

Simultaneously, stakeholder expectations regarding timely and continuous assurance are intensifying [2]. Audit committees, boards of directors, and regulators increasingly view internal audit as a source of early risk signals, rather than solely as a tool for retrospective control.

The transition to near real time auditing occurs within an increasingly complex cybersecurity landscape. Organizations face sophisticated threats to data integrity, system availability, and information confidentiality that traditional periodic audit approaches cannot adequately address [4].

1.2. Research Gap

Prior research has predominantly focused on technical implementation aspects while neglecting the strategic, organizational, and governance prerequisites for sustainable adoption. In particular, limited attention has been paid to the interaction between audit governance, cybersecurity controls, and data governance infrastructures required for near real time assurance. Existing studies frequently address these dimensions separately, which complicates the development of a coherent managerial framework capable of supporting continuous assurance in complex digital environments.

1.3. Theoretical Foundation

This study draws on two complementary theoretical perspectives: Agency Theory provides the foundational rationale for internal audit's monitoring function, explaining how principals (boards, shareholders) demand assurance mechanisms to reduce information asymmetry [11]. Within the proposed framework, Agency Theory explains the demand for enhanced monitoring mechanisms under conditions of information asymmetry, while Institutional Theory explains the organizational processes through which new audit practices become formalized and legitimized. Institutional Theory explains how organizations adopt and legitimize new practices through isomorphic pressures: coercive, mimetic, and normative [12].

1.4. Research Objectives

The aim of the study is to develop a strategic logic for managing the internal audit function during the transition to a near real time mode and to combine key elements into a unified framework model for heads of internal audit in large organizations.

1.5. Contribution

The scientific and practical contribution lies in proposing an applied strategic model based on observed results of internal audit transformation. The scientific novelty consists in viewing the transition as a managerial rather than technological transformation, grounding the framework in Agency Theory and Institutional Theory, and integrating information security considerations.

2. MATERIALS AND METHODS

2.1. Research Design and Analytical Approach

The study is theoretical in nature and aims to develop and substantiate a strategic framework model for managing the transition of the internal audit function to a near real time mode. Empirical experiments and statistical hypothesis testing are not conducted in this work.

The analytical procedure consisted of three stages. First, a structured review of recent academic literature on continuous auditing, cybersecurity governance, and data driven assurance models was conducted. Second, thematic synthesis was applied to identify recurring managerial and technological components associated with near real time auditing practices. Third, the identified components were integrated into a conceptual framework model structured as a multi layer architecture reflecting governance, technological, and organizational dimensions of audit transformation.

The study by Aladwey & El Sayad [1] shows that the transition to continuous reviews is driven by a demand for timeliness but is limited by a lack of standards and independence risks. Almaqtari [2] substantiates that the sustainability of audit digitalization requires a developed IT governance system. Binh [3] records a shift toward data driven models alongside increased significance of information security. Ferreira et al. [4] show that under cyber risk conditions, periodic reviews yield to constant control.

Additional foundational literature: Jensen and Meckling [11] established the agency theoretic rationale for monitoring mechanisms. DiMaggio and Powell [12] provided the institutional framework. Vasarhelyi and Halper [13] conceptualized continuous auditing. The NIST Cybersecurity Framework [17] and ISO 27001 [18] provide guidance on information security controls.

Several limitations bound this study: (1) theoretical nature requires empirical validation; (2) benchmarks derive from specific contexts; (3) assumes baseline data infrastructure maturity; (4) focuses on large organizations.

3. RESULTS

3.1. Drivers, Barriers, and Independence Risks

The conducted analysis indicated that the transition of the internal audit function to a continuous mode is not a linear consequence of technological development, but forms as a result of the sustained interaction of managerial incentives, institutional constraints, and independence loss risks [1].

Analysis shows that the main source of change is external demand for assurance timeliness [5]. Consistent with Agency Theory, this demand originates from principals seeking to reduce information asymmetry [11]. Institutional Theory explains the isomorphic pressures reinforcing this demand [12].

A critical finding relates to information security barriers frequently underestimated in transformation planning. Continuous auditing requires persistent access to sensitive data, creating potential attack vectors if security controls are inadequate. From an implementation standpoint, organizations typically rely on integrated data infrastructures that combine ERP systems, data

warehouses, and security monitoring tools. Continuous auditing mechanisms operate by extracting transactional data streams from operational systems and applying predefined analytical procedures capable of identifying anomalies, deviations from control parameters, or unusual behavioral patterns. This approach enables auditors to monitor control effectiveness continuously rather than retrospectively. Table 1 systematizes the main implementation triggers, barriers, and independence risks.

Table 1. Drivers, Barriers, and Risks to Independence in the Transition to Continuous Auditing
(Compiled by the author based on [1], with theoretical integration and security dimensions)

Category	Top Priority Factor	Value	Strategic Implication	Theoretical Lens
Drivers	Demand for real time reporting	2.72	External demand determines transition pace	Agency Theory
Drivers	Quality and reliability of financial reporting	2.64	Continuous auditing enhances assurance quality	Agency Theory
Drivers	Cybersecurity and data integrity assurance	2.58	Real time threat detection	Institutional Theory
Barriers	Lack of standards and regulatory guidance	3.65	Need for internal policies and role definition	Institutional Theory
Barriers	High infrastructure and technology costs	3.05	Requirement for business case	Resource Based View
Barriers	Cybersecurity readiness gaps	3.42	Security assessment prerequisite	NIST/ISO 27001
Independence	Role ambiguity in continuous auditing	4.59	Necessity of RACI and operating model	Agency Theory
Independence	Review of previously corrected data	4.32	Self review risk requires prohibitions	IIA Standards
Independence	Design of client systems and controls	4.26	Limitation of IA involvement in builds	IIA Standards
Differences	Big Four vs. non Big Four perception	p=0.04	Resource asymmetry during scaling	Contingency Theory

Drivers	Barriers	Independence	Differences

3.2. Practical Benchmarks

During the transition to continuous control loops, audit procedure coverage may expand to levels approaching 100% of relevant transactional populations. Simultaneously, a reduction in cycle time for detecting deviations by more than 60% is observed. These changes are accompanied by a preventative effect estimated at 45 to 50 million AED.

3.3. Thematic Analysis

The thematic distribution of research shows that the largest share of publications is focused on artificial intelligence in auditing [6]. This distribution indicates that technological acceleration in auditing is primarily discussed through AI driven applications, while cybersecurity and access control themes remain less represented despite their critical role in continuous assurance environments. This imbalance supports the need for a more integrated framework combining audit analytics with security and governance safeguards. Figure 1 presents the distribution.

Research Cluster	Share (%)	Strategic Implication
AI in Auditing (core applications)	**34.6%**	AI as foundational infrastructure
Data Security in Auditing	**22.0%**	Cybersecurity prerequisites
Auditing & Accounting Technologies	13.2%	Supporting infrastructure layer
AI & Machine Learning in Auditing	11.5%	Enabling full population analysis
Ethical AI in Audit Systems	8.1%	Accountability requirements
Network Security and Access Controls	6.3%	Security architecture
Other / Emerging Topics	4.3%	Fragmented directions
TOTAL	**100.0%**	

Visual Representation:

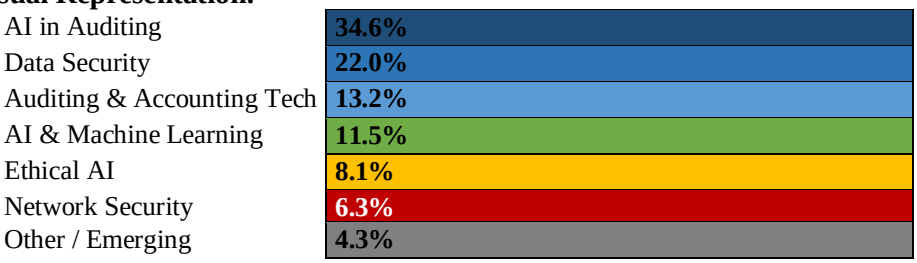


Figure 1. Thematic Structure of AI Based Auditing Research
(Compiled by the author based on [3], percentages recalculated to sum to 100%)

4. DISCUSSION

4.1. Implications for Governance and Audit Leadership

From a network security perspective, internal audit operating in near real time becomes an integral component of the organization's cybersecurity architecture, providing continuous assurance over control effectiveness. In practice, this integration means that internal audit increasingly interacts with security operations centers (SOC), data governance units, and IT risk management teams. Continuous audit monitoring may complement cybersecurity monitoring by providing process level context for detected anomalies. Such integration enhances the organization's ability to identify not only technical security events but also control failures affecting operational and financial processes.

In a near real time environment, the auditor acts not as a reviewer of completed operations, but ensures early deviation detection and dynamic risk assessment. Table 2 compares the traditional and real time models.

Table 2. Strategic Shift of the Internal Audit Function
(Compiled by the author based on [7], with theoretical integration and security dimension)

IA Dimension	Traditional Model (Ex Post)	Real Time Model (AI Driven)	Theoretical Explanation
Time focus	Periodic, after the fact	Continuous, near real time	Reduced information asymmetry (Agency)
Data scope	Sample based testing	Full population analysis	Enhanced monitoring intensity
Auditor's role	Compliance checker	Risk analyst and advisory signal provider	Value added positioning (Institutional)
Nature of assurance	Retrospective confirmation	Ongoing risk oriented assurance	Proactive risk identification
Managerial value	Reactive, limited decision support	Proactive, decision relevant insights	Strategic advisory function
Decision support	Delayed and episodic	Timely and continuous	Real time intelligence
Security role	Periodic security reviews	Continuous security assurance	Integrated cyber defense
Primary risks	Undetected anomalies due to sampling	Independence risks, algorithm transparency, data governance	New risk categories emerge

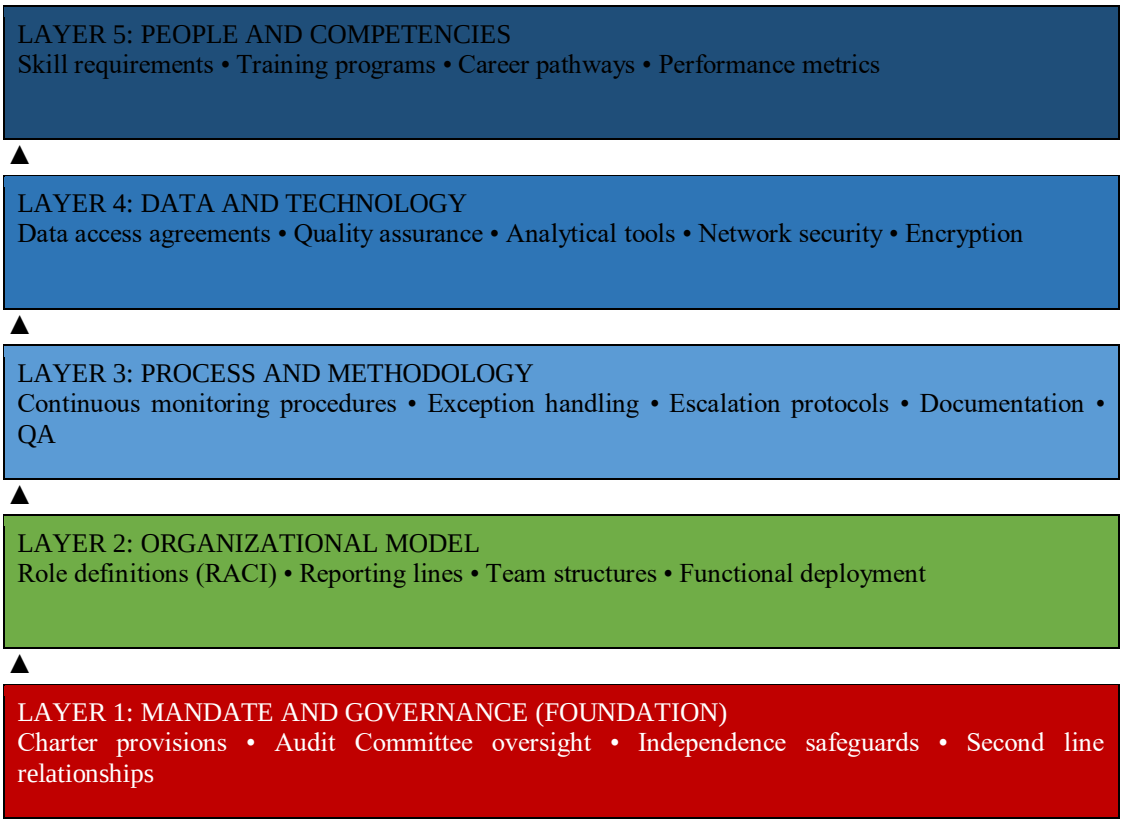
4.2. Reproducibility as Maturity Indicator

Implementation of continuous audit loops represents a managerial task of ensuring repeatability of control actions. The main sign of maturity is a reproducible control loop with predefined frequency, formalized triggers, regulated reaction times, and escalation mechanisms.

Institutional Theory explains this: sustainable practices must be formalized through policies, procedures, and role definitions to achieve legitimacy and persistence [12].

4.3. Framework Architecture

The proposed framework comprises five interdependent layers developed sequentially, as presented in Figure 2.



Note: Layers must be developed sequentially from bottom to top. Attempting to implement upper layers without establishing lower layers leads to fragmentation and sustainability issues.

Figure 2. Five Layer Framework Architecture for Near Real Time Internal Audit
(Proposed by the author)

Each layer of the framework performs a distinct function in enabling near real time auditing. The organizational model layer defines reporting lines, role boundaries, and functional responsibilities. The process and methodology layer formalizes continuous monitoring procedures, exception handling, escalation rules, and quality assurance routines. The data and technology layer provides access to reliable data, analytical tools, encryption, and network security controls. The people and competencies layer ensures that the function possesses the skills, training pathways, and performance mechanisms required for sustainable implementation.

The sequential development of these layers supports the reproducibility and long term stability of the continuous auditing model.

From a theoretical perspective, Layer 1 reflects Agency Theory because it establishes authority, reporting independence, and assurance legitimacy in response to principal demand for reliable oversight. Layers 2 and 3 reflect Institutional Theory because they formalize roles, procedures, and escalation routines through which near real time auditing becomes embedded in organizational practice. Layers 4 and 5 operationalize these foundations through technological capability and human competence.

5. IMPLICATIONS FOR PRACTICE

An illustrative implementation example can be observed in large financial institutions where near real time auditing is applied to procurement and payment processes. Transactional data from ERP systems are continuously analyzed using predefined control rules that detect unusual payment patterns, deviations from authorization hierarchies, or duplicate vendor transactions. Alerts generated by these procedures are reviewed by internal auditors, enabling rapid intervention and preventing potential financial losses. Such applications demonstrate how continuous monitoring mechanisms can enhance both risk detection speed and control effectiveness.

5.1. For Chief Audit Executives

Second, define boundaries explicitly between continuous monitoring (management) and continuous auditing (internal audit). Third, network security cannot be an afterthought. Fourth, invest in competency development. Fifth, establish success metrics.

5.2. For Audit Committees

Significant shifts require Audit Committee endorsement through charter amendments. Committees should ensure continuous auditing responsibilities are authorized and independence safeguards documented. As real time data access increases, self review threats intensify, requiring regular independence reporting.

5.3. For Information Security Professionals

Continuous auditing requires collaboration between internal audit and security teams to design access controls and establish data protection protocols. Internal audit's monitoring can complement SOC activities by providing business process context to security alerts.

6. CONCLUSION

6.1. Summary

Strategic management of the internal audit function during transition to near real time mode represents primarily a task of managing mandate roles, data governance loops, competency development, and independence protection mechanisms. Drawing on Agency Theory and Institutional Theory, transformation success requires simultaneous attention to stakeholder demand alignment and formal institutionalization of new practices.

6.2. Recommendations

The primary stage should be design of the organizational model including responsibility distribution and independence mechanisms. The five layer framework architecture provides a roadmap for sequencing transformation initiatives with security considerations embedded across all layers.

REFERENCES

[1] L. M. A. Aladwey and S. E. Sayad, "Auditors' perceptions of continuous auditing," *Journal of Risk and Financial Management*, vol. 17, no. 12, p. 578, 2024. doi: 10.3390/jrfm17120578

[2] F. A. Almaqtari, "IT governance in AI integration," *Economies*, vol. 12, no. 8, p. 199, 2024. doi: 10.3390/economies12080199.

[3] N. T. T. Binh, "Transforming auditing in the AI era," *Information*, vol. 16, no. 5, p. 400, 2025. doi: 10.3390/info16050400.

[4] L. V. A. Ferreira, R. Silva, and M. A. Santos, "Internal audit strategies for cybersecurity controls," *Applied Sciences*, vol. 15, no. 10, p. 5715, 2025. doi: 10.3390/app15105715.

[5] B. A. F. Jarah, A. M. Alsharairi, and K. A. Alslehat, "Internal audit and creative accounting," *International Journal of Financial Studies*, vol. 10, no. 3, p. 60, 2022. doi: 10.3390/ijfs10030060.

[6] S. D. Lampropoulos, G. P. Koufopoulos, and A. G. Anastasiadis, "Internal audit in ESG implementation," *International Journal of Financial Studies*, vol. 13, no. 4, p. 194, 2025. doi: 10.3390/ijfs13040194.

[7] D. Leocádio, J. C. Ferreira, and M. A. da Silva, "AI in auditing: A conceptual framework," *Administrative Sciences*, vol. 14, no. 10, p. 238, 2024. doi: 10.3390/admsci14100238.

[8] B. Mashayekhi and Y. Mohammed, "Perceived internal audit quality and its determinants," *Journal of Risk and Financial Management*, vol. 18, no. 1, p. 3, 2025. doi: 10.3390/jrfm18010003.

[9] M. Minkkinen, L. Kaivo-oja, and J. Minkkinen, "Continuous auditing of artificial intelligence," *Digital Society*, vol. 1, p. 21, 2022. doi: 10.1007/s44206-022-00021-4.

[10] P. Nkansa, J. K. Appiah, and E. K. Agyei, "Internal audit in enterprise risk management," *Journal of Risk and Financial Management*, vol. 18, no. 12, p. 707, 2025. doi: 10.3390/jrfm18120707.

[11] M. C. Jensen and W. H. Meckling, "Theory of the firm: Managerial behavior, agency costs and ownership structure," *Journal of Financial Economics*, vol. 3, no. 4, pp. 305–360, 1976. doi: 10.1016/0304-405X(76)90026-X.

[12] P. J. DiMaggio and W. W. Powell, "The iron cage revisited: Institutional isomorphism and collective rationality," *American Sociological Review*, vol. 48, no. 2, pp. 147–160, 1983. doi: 10.2307/2095101.

[13] M. A. Vasarhelyi and F. B. Halper, "The continuous audit of online systems," *Auditing: A Journal of Practice & Theory*, vol. 10, no. 1, pp. 110–125, 1991.

[14] Basel Committee on Banking Supervision, *The Internal Audit Function in Banks*, Bank for International Settlements, Basel, Switzerland, 2012. [Online]. Available: https://www.bis.org/publ/bcbs223.htm

[15] J. Kokina and T. H. Davenport, "The emergence of artificial intelligence: How automation is changing auditing," *Journal of Emerging Technologies in Accounting*, vol. 14, no. 1, pp. 115–122, 2017. doi: 10.2308/jeta-51730.

[16] K. C. Moffitt, A. Rozario, and M. A. Vasarhelyi, "Robotic process automation for auditing," *Journal of Emerging Technologies in Accounting*, vol. 15, no. 1, pp. 1–10, 2018. doi: 10.2308/jeta-10589.

[17] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg, MD, USA, 2018. [Online]. Available: https://www.nist.gov/cyberframework

[18] International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection*, ISO, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/27001

[19] Institute of Internal Auditors, *Global Internal Audit Standards*, IIA, Altamonte Springs, FL, USA, 2024. [Online]. Available: https://www.theiia.org/en/standards

[20] Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework*, COSO, New York, NY, USA, 2013. [Online]. Available: https://www.coso.org

[21] M. H. Christ, M. L. Ege, and T. A. Sedatole, "Rotational internal audit programs and financial reporting quality," *Accounting, Organizations and Society*, vol. 44, pp. 37–59, 2015. doi: 10.1016/j.aos.2015.04.001.

[22] S. Ramamoorti, *Internal Auditing: History, Evolution, and Prospects*, Institute of Internal Auditors Research Foundation, Altamonte Springs, FL, USA, 2003.