INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 15, Issue 12, (2025) E-ISSN: 2222-6990

Auditing Artificial Intelligence in Practice: Insights from Internal Auditors on Risk, Adoption, and Assurance

Doong Yee Jiun[1,2], Ramli Razli[2]

[1]Heytap Pte Ltd, Singapore, [2]Azman Hashim International Business School, Universiti Teknologi Malaysia, Malaysia

Corresponding Author Email: razli@utm.my

DOI Link: http://dx.doi.org/10.6007/IJARBSS/v15-i12/27149

Published Date: 23 December 2025

Abstract

This study investigates how internal audit functions are responding to the adoption of artificial intelligence (AI) and how they are incorporating AI-related risks into their assurance and governance practices. It applies institutional theory to examine how regulatory, resource, and normative pressures shape audit responses in emerging economies. A qualitative, exploratory approach was used involving a focus group of six senior internal audit managers from various Malaysian industries. Manual transcription and inductive thematic coding were applied to identify key themes relating to AI risk integration, audit execution, and governance practices. The analysis revealed four major themes: (1) early-stage AI governance is shaped by symbolic compliance and increasing regulatory expectations; (2) limited technical capability and audit resources hinder audit maturity; (3) frameworks such as ISACA, NIST, and ISO are commonly referenced but must be adapted to context; and (4) internal audit functions are shifting toward a strategic advisory role, particularly in technology-forward organizations. Tensions between innovation and control were noted across sectors. Findings are context-specific to Malaysia and reflect the early maturity stage of AI audit practice. Future research should explore cross-country comparisons and longitudinal developments as audit practices evolve. This study contributes to the emerging literature on AI governance by providing rich field-based evidence of how internal auditors interpret and operationalize AI risk. It advances institutional theory within the auditing context and offers practical insights for regulators, professional bodies, and assurance leaders navigating AI adoption.

Keywords: Artificial Intelligence Auditing, AI Risk Assurance, Internal Audit, AI Risk Management, Technology Governance

Introduction

Artificial intelligence (AI) is reshaping the institutional architecture of contemporary organizations, transforming not only how business functions are executed, but also how

decisions are justified, governed, and held accountable. Once regarded as experimental tools, AI technologies ranging from predictive analytics and autonomous decision engines to generative applications such as ChatGPT have become embedded organizational infrastructure. Recent estimates indicate that 72% of global firms have adopted AI in at least one business function, with more than half deploying AI across multiple functions, reflecting a rapid acceleration in adoption (Forbes, 2024; Haan, 2024). While these technologies promise efficiency, scalability, and innovation, they simultaneously generate profound governance challenges, including algorithmic opacity, data bias, ethical ambiguity, and fragmented accountability structures (Ashta & Herrmann, 2021). These challenges raise fundamental questions about how organizations demonstrate control, responsibility, and legitimacy in AI-driven environments.

Within this context, internal audit occupies a critical yet increasingly complex governance role. Traditionally positioned as a retrospective assurance function, internal audit is now expected to provide forward-looking oversight over AI systems that are probabilistic, adaptive, and often non-transparent by design. Unlike legacy information systems, AI technologies frequently lack stable rules, clear audit trails, and standardized control mechanisms, rendering conventional audit approaches insufficient. Consequently, the remit of internal audit is expanding beyond compliance validation to encompass emerging technology risks, ethical considerations, and governance assurance (Wassie & Lakatos, 2024). However, audit readiness for this expanded role remains uneven. Skills shortages, limited resources, and reliance on outdated risk frameworks contribute to growing "assurance gaps," wherein AI-related risks are acknowledged in principle but inadequately addressed in practice within organizational control systems.

These tensions are particularly salient in emerging economies such as Malaysia, where the state has adopted an ambitious, policy-led approach to digital transformation. Initiatives such as the Malaysia National AI Roadmap (2021–2025) and the MyDIGITAL Blueprint explicitly promote AI adoption across key industries and public sector governance. Yet, despite strong policy momentum, the institutional infrastructure required to regulate, govern, and audit AI systems remains underdeveloped (Artificial Intelligence Roadmap 2021–2025, 2023; Malaysia Digital Economy Blueprint, 2021). The national AI governance framework is still in draft form, and coordination between external regulatory expectations and internal governance functions particularly internal audit remains limited. This regulatory ambiguity creates a critical space in which organizations must interpret, negotiate, and respond to AI governance demands without clear enforcement or assurance standards.

To examine how such responses unfold, this study adopts neo-institutional theory as its analytical lens. Neo-institutional theory suggests that organizational practices are shaped not solely by efficiency considerations, but also by legitimacy-seeking behaviour under conditions of uncertainty, professional norms, and regulatory pressure. This perspective is especially relevant in the context of AI governance, where organizations may adopt formal structures, policies, or references to international frameworks as signals of conformity, even when underlying practices and capabilities remain underdeveloped. Internal audit, positioned at the intersection of technical control and institutional legitimacy, plays a pivotal role in mediating these pressures, translating external expectations into organizational practice or, in some cases, symbolic compliance.

Despite growing scholarly interest in AI governance and ethical frameworks, empirical research examining how internal audit functions engage with AI-related risks remains limited, particularly in emerging market contexts. Existing studies tend to focus on normative frameworks, regulatory design, or technical risk categories, offering limited insight into how audit practitioners interpret and operationalize AI governance under real-world constraints. Addressing this gap, the present study draws on a qualitative focus group involving six senior internal audit managers from diverse Malaysian industries to explore three core issues: (1) the extent to which AI-related risks have been formally integrated into enterprise risk registers; (2) whether AI audit activities have been conducted or planned; and (3) how internal auditors perceive, adopt, or adapt international AI governance frameworks, such as those issued by ISACA and NIST, within resource-constrained organizational settings.

By reframing internal audit's role in the age of AI as a socially embedded governance function rather than a purely technical mechanism, this study contributes to the literature on digital risk assurance, accountability, and institutional change. It advances social science debates on legitimacy, symbolic compliance, and governance under uncertainty by demonstrating how assurance gaps emerge when technological adoption outpaces institutional capacity. In doing so, the study offers both theoretical and practical insights into the evolving role of internal audit as organizations navigate the institutional complexity of AI-driven transformation.

Theoretical Framing and Research Questions

The role of internal audit is traditionally framed in technical terms: evaluating internal controls, monitoring compliance, and offering assurance over financial and operational risks. However, the emergence of artificial intelligence (AI) as a pervasive and complex organizational technology calls for a broader conceptual lens, one that considers not only technical capability but also institutional context, legitimacy pressures, and symbolic adoption. To that end, this study draws on neo-institutional theory to interpret how internal audit functions are responding to AI governance demands.

Neo-institutional theory posits that organizations do not adopt new practices purely for functional efficiency, but also to maintain legitimacy in the face of evolving professional norms, stakeholder expectations, and regulatory uncertainty (DiMaggio & Powell, 1983; Meyer & Rowan, 1977). In this view, internal audit's engagement with AI risks may be driven not only by substantive concerns about control effectiveness but also by mimetic, normative, or coercive pressures, such as benchmarking against peers, adopting globally endorsed frameworks, or reacting to loosely defined regulatory signals. This perspective allows for the examination of symbolic compliance, where formal structures (e.g., risk registers or audit frameworks) are adopted to signal alignment with best practice, even when underlying practices or capabilities remain underdeveloped.

This lens is particularly relevant in emerging market contexts, such as Malaysia, where state-led digital transformation agendas, including the *Malaysia National AI Roadmap (2021–2025)* and the *MyDIGITAL Blueprint*, create normative and regulatory pressure for organizations to adopt AI technologies and ensure responsible use. Yet, at the organizational level, internal audit teams may lack the resources, skills, or internal influence to operationalize AI assurance. Institutional theory enables us to interrogate not just whether

audit functions are adopting AI audit practices, but *why*, and to what extent these practices reflect genuine readiness versus symbolic alignment.

Based on this framing, the study is guided by the following research questions:

RQ 1. To what extent have internal audit functions integrated AI-related risks into enterprise risk registers and audit planning processes?
This question explores the formal recognition of AI as a distinct class of risk and how internal audit scopes are adapting in response.

RQ 2. What challenges and constraints do internal auditors face in assessing or auditing AI systems, particularly in terms of skills, resources, and organizational support?
This question investigates internal limitations, technical, cultural, and institutional, that shape audit readiness.

RQ 3. How do internal auditors interpret and engage with global AI audit frameworks (e.g., ISACA, NIST), and what influences their adoption or rejection of these tools?
This question considers whether external frameworks are used substantively or symbolically, and what institutional forces influence their perceived value.

Together, these questions allow for an exploration of how internal audit practices evolve, or are constrained, under conditions of technological innovation and institutional uncertainty. They also reflect a broader interest in how accountability mechanisms are maintained, redefined, or weakened in digitally transforming organizations.

Literature Review

Artificial Intelligence in Organizations

Artificial Intelligence (AI) has rapidly transformed the architecture of organizational decision-making and control (Mohammed & Madhumithaa, 2024). From predictive algorithms to generative tools like ChatGPT, AI systems are now used in domains such as customer service automation, fraud detection, financial forecasting, and compliance monitoring While these technologies improve operational efficiency and responsiveness, they also introduce systemic risks—such as data bias, model opacity, and a lack of explainability, that challenge existing risk governance mechanisms (Al-Hchemi & Haleem , 2024; Anozie et al., 2024) Ashta & Herrmann, 2021; Jassem & Al Balushi, 2025; Puchakayala, 2024).

The deployment of AI in high-stakes decision contexts has raised significant ethical, legal, and technical concerns, particularly in relation to accountability. Scholars warn that organizational adoption of AI often outpaces the development of internal oversight mechanisms (Birkstedt et al., 2023; Ishkhanyan, 2025). For assurance providers such as internal audit, the shift toward AI-governed decision environments necessitates a rethinking of what it means to audit, evaluate, and certify systems whose behaviour may be neither fully predictable nor interpretable (Lacmanovic & Skare, 2025).

AI Governance and Assurance Frameworks

To mitigate the risks posed by AI systems, several global frameworks have been developed to promote responsible, transparent, and accountable AI. These include the NIST AI Risk Management Framework (AI RMF), the ISACA Artificial Intelligence Audit Toolkit, and the ISO/IEC 42001 international standard. Although their structures differ, each framework offers principles and tools to help organizations evaluate AI systems across development, deployment, and governance stages.

- The NIST AI RMF (2023) offers a voluntary, flexible framework organized around four core functions, Map, Measure, Manage, and Govern, while emphasizing principles like fairness, reliability, and inclusiveness. It also introduces a role-based model, identifying key AI ecosystem actors such as developers, operators, and evaluators.
- The ISACA AI Audit Toolkit (2023) is specifically targeted at internal auditors. It structures its assessment around ten control families covering governance, human oversight, data integrity, system lifecycle, incident response, and third-party risks. It supports audit readiness by translating abstract AI risks into concrete control expectations.
- The ISO/IEC 42001 (2023) is the first certifiable international standard for AI management systems. It focuses on governance processes such as leadership, planning, evaluation, and improvement. Its core appeal lies in establishing organizational accountability and auditability for AI system deployment.

Table 2.1
Summary of Key AI Governance Frameworks

Framework	Issuer	Structure / Components	Scope & Audience	Core Principles & Unique Features
NIST AI RMF (2023)	National Institute of Standards & Tech (USA)	Four functions: Map, Measure, Manage, Govern; emphasizes trustworthy AI traits	Policymakers, developers, auditors, regulators	Fairness, accountability, reliability, transparency, and inclusiveness; defines AI system actors (e.g., owners, deployers, users)
ISACA AI Audit Toolkit (2023)	Information Systems Audit and Control Association (Global)	Ten control families: Governance, Human Factors, Data, Performance, Operations, Monitoring, Security & Privacy, System Lifecycle, Third-Party Risk, Incident Management	Internal auditors, IT auditors	Practical audit guidance aligned with COBIT; operationalizes AI assurance; human oversight and lifecycle controls; enables stepby-step audit execution
ISO/IEC 42001 (2023)	International Organization for Standardization (ISO)	Requirements-based structure for AI management systems including planning, support, operations, and performance evaluation	Organizations deploying or developing AI systems	First certifiable AI governance standard; emphasizes risk-based approach, compliance, continual improvement; designed for auditable implementation

(Source: ISACA 2023, NIST 2023, ISO 2023)

Despite their robust design, these frameworks are often under-utilized in practice, particularly in resource constrained or regulation-ambiguous environments. Existing literature has not sufficiently explored how internal auditors engage with these tools, or whether their usage is substantive or symbolic. This study contributes to closing that gap.

The Role of Internal Audit in AI Assurance

As AI reshapes operational and strategic functions, internal audit is increasingly expected to offer assurance not only over traditional IT controls, but also over algorithmic systems. A joint publication between The Institute of Internal Auditors and Wolter Kulwer (2024) highlights AI as a critical risk frontier. Yet, there is limited empirical evidence on how audit functions are adjusting. Studies point to a lack of auditor expertise, limited training programs, and resistance to new audit scopes that demand technical sophistication (Arun, 2024; Hamzah et al., 2024; Manuel & Arumugam, 2024; Ismail et al., 2024).

Furthermore, the ambiguous nature of AI risks, non-deterministic behaviours, continuous learning models, and embedded biases, makes them difficult to evaluate through conventional audit procedures. This creates a mismatch between institutional expectations and actual audit capability. Where frameworks exist, they may be acknowledged but not fully internalized or applied, what Power (1997) calls the “rituals of verification.”

Institutional Theory and Symbolic Assurance

Institutional theory provides a critical lens to examine how organizations adopt assurance frameworks under environmental pressure. DiMaggio and Powell’s (1983) typology of coercive, mimetic, and normative isomorphism explains how external pressures shape internal practices. In the context of AI, organizations may implement audit structures to appear compliant with global standards without substantively altering underlying capabilities, a phenomenon described as *symbolic compliance* (Meyer & Rowan, 1977).

Within internal audit, symbolic engagement with frameworks like ISACA or NIST may fulfil board or regulatory expectations but fall short of enabling meaningful AI risk oversight. Literature in accounting and accountability has emphasized the need to differentiate between “real” and “ritualistic” forms of assurance, especially in settings where professional norms and technical systems evolve faster than organizational readiness (Sikka, 2009).

Research Gaps in Emerging Economies

While governance-oriented literature on AI is growing, it remains disproportionately focused on institutions in North America and Western Europe. Very few studies have examined how internal audit teams in emerging economies engage with AI risk. Malaysia offers a compelling context: it has launched a National AI Roadmap and the MyDIGITAL blueprint to accelerate AI development, yet many organizations remain in early stages of implementation, and internal audit functions face acute resource and skill limitations.

This disconnects between policy ambition and institutional capacity creates a fertile ground to study how audit teams interpret, adapt, or resist global frameworks, offering critical insight into how assurance evolves under transitional digital governance regimes. This study aims to fill that gap through empirical insights from Malaysian audit managers currently facing the pressures and uncertainties of AI integration.

Despite growing attention to AI governance, there remains a lack of field-based evidence on how internal audit functions respond to AI-related risks in practice, particularly outside Western institutional settings. Most existing studies privilege regulatory intentions or technical frameworks, overlooking the lived experiences of audit professionals navigating ambiguous expectations, limited expertise, and competing institutional logics. This study addresses this gap by examining how internal auditors in Malaysia interpret AI governance demands, revealing the tension between symbolic compliance and substantive assurance. By doing so, it contributes to broader social science debates on institutional legitimacy, accountability under uncertainty, and the performative dimensions of governance in digitally transforming organizations.

Methodology

Research Approach and Design

This study adopts an interpretivist, qualitative research approach to explore how internal audit functions interpret and respond to the emerging demands of artificial intelligence (AI) risk governance. Grounded in institutional theory, the study seeks to understand not only what practices internal auditors are adopting but how their actions are shaped by regulatory signals, professional norms, and organizational constraints. Given the exploratory nature of the topic and the under-researched context, a qualitative design was deemed most appropriate.

A single focus group was conducted, involving six senior internal audit professionals from Malaysian organizations with varying degrees of AI exposure. Focus groups are well-suited to uncovering complex reasoning and interactive meaning-making (Barbour, 2007), particularly when the research objective is to surface nuanced perceptions among seasoned professionals. The setting enabled participants to engage, compare perspectives, and collectively articulate challenges and aspirations around AI assurance.

Participant Selection and Context

Participants were selected using purposive sampling based on two criteria: (1) holding a senior role in internal audit, and (2) working in organizations that have either adopted or considered AI in business operations. Participants represented a diverse range of industries, including financial services, manufacturing, technology, healthcare, automotive, and real estate, providing cross-sectoral insights. Table 1 summarizes the participants' roles, organizational audit structure, and AI audit readiness.

Table 3.1
Participant Profile and AI Audit Engagement

Code	Position	Industry	Audit Model	IT Audit Team	AI in Audit Scope	Exploring AI
P1	Vice President	Financial Services	Co-source	Yes	Yes	Yes
P2	Audit Director	Manufacturing	In-house	Yes	No	Yes
P3	Senior Audit Manager	Technology	Co-source	Yes	No	Yes
P4	Senior Audit Manager	Healthcare	Co-source	No	No	No
P5	Audit Manager	Automotive	Co-source	No	No	No
P6	Audit Manager	Real Estate & Construction	In-house	Yes	No	No

Data Collection and Ethics

The focus group was conducted virtually and lasted approximately 90 minutes. A semi-structured guide was used to facilitate discussion around four core themes: AI risk governance, inclusion in the risk register, current or planned audit activities, and perceived barriers to AI assurance. The discussion was audio recorded with participants' consent and manually transcribed by the researcher. Both verbal and written consent were obtained from all participants prior to the session. The study did not require formal institutional ethical clearance, but all ethical research principles were followed, including voluntary participation, data confidentiality, and anonymization of participant identities.

Data Analysis

Data was analysed using a manual thematic analysis approach following Braun and Clarke's (2006) six phase method. The analysis began with familiarization through repeated readings of the transcript, followed by two iterative rounds of coding:

- The first coding cycle used inductive open coding, allowing patterns to emerge from the data itself without imposing a predetermined structure.
- The second cycle involved grouping initial codes into broader themes aligned with institutional theory constructs such as coercive pressures, symbolic compliance, capacity constraints, and normative professional resistance.

Themes were refined through multiple iterations, with codes re-evaluated for consistency and thematic coherence. Given the focus group's interactive dynamic, attention was also paid to consensus and divergence among participants' views.

Researcher Positionality and Reflexivity

The lead researcher is a seasoned internal audit professional with over 12 years of experience across both second and third lines of defense, having held leadership roles in

compliance, internal audit, and consultancy. This professional background facilitated trust and rapport during data collection and enabled deeper contextual interpretation of participant narratives. However, reflexivity was maintained throughout the process to minimize the risk of professional bias and to ensure that participant voices remained central to the analysis.

Finding and Thematic Analysis

Drawing on focus group data from six internal audit managers in Malaysia, this section presents four major themes that emerged from the thematic analysis. These findings are interpreted through the lens of institutional theory, highlighting how coercive pressures, resource constraints, and professional norms shape internal audit responses to AI risk.

Navigating Early-Stage AI Governance Amid Regulatory Pressure

Participants reported growing awareness of AI-related risks and acknowledged increasing regulatory expectations. Several organizations have started integrating AI into risk registers, often classifying it under broader categories such as technology or cybersecurity risk. Notably, organizations in regulated industries, such as financial services and manufacturing, appeared more proactive.

"We documented AI risk in our risk register, especially after learning our statutory auditor plans to expand their tech audit coverage to AI. The CISO and cybersecurity team currently own the risk." (P1)

"We haven't listed AI in the risk register yet, but we're covering AI as part of audits on related systems, like supply chain automation." (P2)

"We were told that our statutory auditor will include AI auditing in upcoming reviews, but we have no clue what exactly they will do. At least ISACA, NIST, and ISO frameworks give us a solid reference to align and defend our approach." (P1)

Regulatory visibility, such as expectations from central banks or statutory auditors, served as coercive pressure prompting audit functions to act. However, the depth of risk formalization varied across sectors, reflecting institutional uncertainty and evolving norms. Frameworks like ISACA, NIST, and ISO were commonly referenced as foundations, especially for tailoring audit programs in regulated industries.

"Each framework offers a good baseline, but they all need customization depending on the industry, especially when we have to account for sector-specific regulations." (P1)

Capacity and Capability Constraints in AI Audit Execution

All participants emphasized significant talent and resource gaps in planning and executing AI audits. Even firms with mature IT audit functions struggled with a lack of specialized AI audit knowledge, compounded by budget constraints and high costs of external expertise.

"We developed our own RCM and audit program, but it took years to build. Skilled professionals are limited in Malaysia, and it's been tough even to hire IT auditors." (P1)

"Even our co-source partner, a Big Four firm, admitted they weren't confident auditing AI. That stalled our plans to start." (P3)

"There's already excessive workload from conventional audits. Adding AI would further burden both internal audit and IT." (P2)

Participants shared efforts to overcome these barriers through training and recruitment strategies. Several audit teams have shifted their hiring preference from accounting-only profiles to include more candidates with IT backgrounds, in response to pressure from audit committees.

"Our Audit Committee constantly pushes for integrated audit teams, audit automation, and continuous auditing—so we've expanded our recruitment scope beyond accounting graduates." (P3)

The lack of market maturity in AI audit training and tools was a recurring challenge. Participants expressed a desire for more local, practitioner-oriented workshops, especially from professional bodies like ISACA and IIA.

Symbolic Compliance vs Substantive Engagement

The data revealed contrasts between superficial engagement with AI audit expectations and more structured efforts. Some organizations-initiated discussions or registered AI risks without taking further action, reflecting symbolic assurance. Others had begun substantive work, such as developing internal audit programs based on international frameworks.

"We're still exploring what to audit. For now, we just make sure to discuss security and accuracy during audit." (P2)

"We thought of auditing AI, but no clear path and no capable partner—so we postponed." (P3)

"Our audit committee expects us to self-detect issues before external assessors do. That's why we moved early and involved ourselves from the development phase." (P1)

Additionally, participants noted that while frameworks like ISACA, NIST, and ISO are helpful, their effectiveness relies on how well they are adapted to context and used proactively.

"ISACA, NIST and ISO give us a good foundation, especially to build audit programs that can stand up during statutory audits. It's better than just using generic sources." (P2)

These patterns align with Meyer and Rowan's (1977) view of ceremonial conformity: organizations mimic best practices under pressure but struggle to embed them meaningfully. In some sectors, symbolic conformity prevailed due to competing high-risk priorities and limited audit influence.

"In healthcare, DOJ penalties have forced us to focus on compliance risks. AI may be important, but we're currently focused on areas with clearer regulatory exposure." (P4)
"It's tough to challenge business if we can't quantify the risk. Many prefer to react only after damage is done." (P2)

The Expanding Role of Internal Audit in AI Governance

Several participants described a shift in internal audit's role, from assurance provider to strategic advisor. In some cases, internal auditors were part of AI steering committees or played a role in co-developing governance structures.

"Before the AI tool is finalized, we're working closely with the AI team. It's more of a strategic partnership now." (P5)
"We've become more agile, involved earlier in development. That's crucial for a regulated industry like ours." (P1)

Participants from technology-focused and fast-paced industries reported the tension between enabling AI driven innovation and maintaining sufficient governance.

"In our industry, AI is a key efficiency driver. The challenge is finding balance governance versus innovation especially when auditors aren't yet fully skilled." (P3)

While still limited, this evolution reflects internal audit's potential to support ethical AI deployment beyond traditional controls testing. Participants emphasized the need for agility, learning, and integration into innovation processes.

*"Internal audit must evolve. The journey is tough, but starting early matters." (*P1)

These insights suggest that internal audit's contribution to AI governance is not just a matter of competence, but also positioning within the broader organizational structure and its relationships with business units and the second line of defence.

Discussion

The findings illustrate how internal audit functions are navigating AI adoption within dynamic institutional environments shaped by regulatory signals, resource constraints, and evolving professional expectations. By applying institutional theory, we can better understand the patterns of engagement, resistance, and symbolic adaptation observed across organizations.

First, consistent with the concept of coercive isomorphism (DiMaggio & Powell, 1983), many participants described the influence of statutory auditors, financial regulators, and sector-specific compliance obligations as key drivers for considering AI in the risk register and audit scope. In heavily regulated sectors like financial services and healthcare, external scrutiny and past enforcement experiences heightened pressure for early integration. This coercion, however, was unevenly translated into action. Some participants viewed frameworks such as ISACA and NIST not only as compliance tools but also as strategic resources to align with regulatory expectations, especially when facing ambiguity from external assessors. Second, findings related to capability constraints align with prior studies

showing how audit innovation is hampered by skills shortages, budget limitations, and tool immaturity (Rahman et al., 2021). The Malaysian context amplifies these challenges due to the limited availability of localized training and practitioner resources. Although audit committees are pushing for integrated teams and automation, progress is uneven. This suggests that technical readiness alone is insufficient, professional infrastructure and sectoral maturity matter equally.

Third, the presence of symbolic compliance, where AI risk is acknowledged but not fully operationalized, mirrors broader critiques of performative governance (Power, 2007). In some organizations, AI risks were included in risk registers or discussed during audits without leading to meaningful audit activities. This behaviour reflects a decoupling between policy and practice and is often driven by uncertainty, lack of auditability, and prioritization of more immediate risks such as statutory compliance and enforcement penalties (especially in healthcare and manufacturing). Fourth, a key contribution lies in the observation of organizational tensions between innovation and assurance. Participants from fast-paced industries like technology emphasized that audit's lack of AI fluency can conflict with business imperatives to innovate. Internal audit functions are thus caught between enabling digital transformation and fulfilling their governance mandate. This mirrors the duality of institutional logic, balancing market efficiency with risk accountability.

"Everyone wants the business to move fast and stay competitive… we work hard with compliance and legal to strike a balance." (P3)

This tension has theoretical significance. It reflects the limits of isomorphic pressure when multiple logics (innovation vs. control) compete within the same institutional field. Lastly, the findings show signs of a professional identity shift. Several participants described how internal audit is increasingly engaged earlier in AI system development and is expected to provide advisory input rather than solely post-facto assurance. This aligns with Roussy et al. (2020)'s perspective on the hybrid role of internal audit as both a compliance actor and a facilitator of organizational learning. However, this transformation is fragile. Without adequate resources, audit teams risk becoming symbolically involved but substantively underpowered.

Together, these findings contribute to the literature by demonstrating that AI audit engagement is not simply a function of technical readiness but is mediated by institutional logic, organizational power dynamics, and the broader socio-regulatory landscape. This study also underscores the importance of contextual capacity building in emerging markets to bridge the gap between rhetoric and reality in AI assurance practices.

Practical Implications and Limitations

Practical and Policy Implications

The study's insights have meaningful implications for regulators, professional bodies, and internal audit functions:

Table 6.1
Key Practical and Policy Implications for Internal Audit Stakeholders in AI Governance

Stakeholder Group	Implication
Internal Audit Leaders	Diversify team skillsets, engage early in AI development, and enhance agility to influence innovation governance.
Regulators & Statutory Auditors	Define clearer expectations and auditability standards for AI-related risks to reduce ambiguity and promote consistent audit engagement.
Professional Associations	Develop and deliver regional, context-sensitive training programs (e.g., through ISACA and IIA) to build AI audit capabilities in emerging markets.

Limitations and Directions for Future Research

While this study offers rich qualitative insight, it is limited to six senior professionals within the Malaysian context, which may constrain generalizability. Future studies could:

- Extend the research to other emerging markets or comparative jurisdictions.
- Explore cross-functional dynamics between internal audit, IT, and compliance in AI governance.
- Conduct longitudinal studies to assess how symbolic or substantive audit practices evolve over time as AI technologies mature.

Despite these limitations, this research contributes timely insights into the evolving nature of internal audit in the face of emerging technology governance challenges.

Conclusion

This study explored how internal audit functions in Malaysia are responding to the governance and risk assurance challenges posed by artificial intelligence. Drawing on focus group data and guided by institutional theory, the findings reveal a field in flux, characterized by early-stage engagement, regulatory influence, capability gaps, and an emerging shift in audit role identity. Theoretically, the study advances understanding of how institutional logics shape audit practice in response to emerging technologies. It contributes to the literature by showing how symbolic compliance and substantive assurance coexist within the same organizations, reflecting both external pressures and internal capacity gaps. Practically, the findings suggest that internal audit functions must balance agility with prudence: becoming early collaborators in AI development while also advocating for structured guidance, resources, and professional development. For policymakers and standard-setters, the results underscore the need for clearer regulatory signals and localized capacity building. For professional bodies, such as ISACA and IIA, the findings point to a strong demand for region-specific, practice-oriented training and tools. In conclusion, internal audit's journey into AI governance is just beginning. Whether this journey results in genuine assurance or symbolic alignment will depend on how the profession adapts its structures, capabilities, and institutional relationships in the face of rapid technological change.

References

Al-Hchemi, & Haleem, L. (2024). Evaluating Generative AI in enhancing banking services efficiency. Economic Forum, 14(4), 47–54. https://doi.org/10.62763/ef/4.2024.47

Anozie, C., Barnabas, O., Chukwuemeka, P., Adeleke, N., Ukadike, A., & None Omodunni Adejoke Oloko. (2024). Advancements in artificial intelligence for omnichannel marketing and customer service: Enhancing predictive analytics, automation, and operational efficiency. International Journal of Science and Research Archive, 12(2), 1621–1629. https://doi.org/10.30574/ijsra.2024.12.2.1436

Artificial Intelligence Audit Toolkit. (2023). ISACA. https://store.isaca.org/s/store#/store/browse/detail/a2S4w000007kB9pEAE

Artificial Intelligence Roadmap 2021-2025. (2023, December 1). Malaysian Science and Technology Information Centre. https://mastic.mosti.gov.my/publication/artificial-intelligence-roadmap-20212025/

Arun, K. (2024). ARTIFICIAL INTELLIGENCE AND INTERNAL AUDIT STAFFING PRACTICES: NECESSITATING A DIFFERENT SKILL SET FROM AUDITORS. Denetişim. https://doi.org/10.58348/denetisim.1519491

Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. Strategic Change, 30(3), 211–222. https://doi.org/10.1002/jsc.2404

Barbour, R. (2007). Doing Focus Groups. London: SAGE Publications.

Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: themes, knowledge gaps and future agendas. Internet Research, 33(7), 133–167. https://doi.org/10.1108/intr-01-20220042

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101

Haan, K. (2024, June 15). 24 Top AI Statistics & Trends in 2023 (R. Watts, Ed.). Forbes. https://www.forbes.com/advisor/business/ai-statistics.

Hamzah, P., Yeba, E., Maithy, S. P., & Poetra, G. B. (2024). Opportunities and Challenges in IntegratingArtificial Intelligence into Financial Auditing. Journal of Economic Education and Entrepreneurship Studies, 5(4). https://doi.org/10.62794/je3s.v5i4.4563

Harnessing Generative AI for internal audit activities. (2024). Wolters Kluwer Financial Services, Inc. https://www.theiia.org/globalassets/site/content/research/foundation/2024/harnessinggenerativeai_1. pdf

Ishkhanyan, A. (2025). Governing AI across borders: corporate power, state sovereignty and global regulation. Digital Policy Regulation and Governance. https://doi.org/10.1108/dprg-03-2025-0057 Ismail, M. K. A. H., Rajiun, A. A. M. A., Kamal, S. S. B. M., Azmidal, N. I., Nizam, N. I. S., Yussop, N. D. I. M., Jamil, M. M., & Deraman, N. A. (2024). AI-Powered Internal Auditing: Transforming the Profession for a New Era. International Journal of Research and Innovation in Social Science, VIII(X), 2406–2413. https://doi.org/10.47772/ijriss.2024.8100199 ISO/IEC 42001:2023. (2023). ISO. https://www.iso.org/standard/42001

Jassem, S., & Al Balushi, W. (2025). ChatGPT and Implications for the Banking and Financial Industry: New Horizons of Opportunities and Potential Perils. The ChatGPT Revolution, 183–202. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83549-852-120251009

Lacmanovic, S., & Skare, M. (2025). Artificial intelligence bias auditing – current approaches, challenges and lessons from practice. Review of Accounting and Finance, 24(3). https://doi.org/10.1108/raf-012025-0006

Malaysia Digital Economy Blueprint. (2021, February 19). ECONOMIC PLANNING UNIT, PRIME MINISTER'S DEPARTMENThttps://ekonomi.gov.my/sites/default/files/2021-02/malaysiadigital-economy-blueprint.pdf

Manuel, A., & Arumugam, S. K. (2024). Harnessing Artificial Intelligence in Internal Auditing. Advances in Business Information Systems and Analytics Book Series, 95–114. https://doi.org/10.4018/979-83693-4187-2.ch005

Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550

Mohammed, I. A., & Madhumithaa, N. (2024). Transforming Decision Making: The Impact of AI and Machine Learning on Strategic Business Operations. Library Progress International, 44(3), 22005– 22013.

National Institute of Standards and Technology. (2023, July 12). AI Risk Management Framework. NIST. https://www.nist.gov/itl/ai-risk-management-framework

Power, M. (1997). The audit society: Rituals of verification. Oxford University Press.

Puchakayala, P. R. A. (2024). Generative Artificial intelligence Applications in Banking and Finance sector. World Journal of Advanced Research and Reviews, 23(1), 3105–3120. https://doi.org/10.30574/wjarr.2024.23.1.1999

Rahman, F., Putri, G., Wulandari, D., Pratama, D., & Permadi, E. (2021). Auditing in the Digital Era: Challenges and Opportunities for Auditor. Golden Ratio of Auditing Research, 1(2), 86–98. https://doi.org/10.52970/grar.v1i2.367

Roussy, M., Barbe, O., & Raimbault, S. (2020). Internal audit: from effectiveness to organizational significance. Managerial Auditing Journal, 35(2), 322–342. https://doi.org/10.1108/maj-01-20192162

Sikka, P. (2009). Financial crisis and the silence of the auditors. Accounting, Organizations and Society, 34(6-7), 868–873. https://doi.org/10.1016/j.aos.2009.01.004

Wassie, F. A., & Lakatos, L. P. (2024). Artificial intelligence and the future of the internal audit function. Humanities and Social Sciences Communications, 11(1). https://doi.org/10.1057/s41599024-02905-w