

Auditing AI in 2025: Building an AI-enabled Internal Audit Function under the new IIA Standards

Purpose: This paper examines how internal audit functions can safely integrate Artificial Intelligence (AI) into their practices in 2025, aligning with the 2024 Global Internal Audit Standards (effective January 2025) and mapping to emerging AI governance frameworks (ISO/IEC 42001 and NIST AI RMF).

56 min read • 12 sections • LISRC R&D practice



LISRC Research & Development

The applied-research practice of London International Studies & Research Centre

01 Abstract

Purpose: This paper examines how internal audit functions can safely integrate Artificial Intelligence (AI) into their practices in 2025, aligning with the 2024 Global Internal Audit Standards (effective January 2025) and mapping to emerging AI governance frameworks (ISO/IEC 42001 and NIST AI RMF). We provide a framework for an AI-enabled internal audit function covering the audit lifecycle—planning, fieldwork, and reporting—while ensuring trust, ethics, and compliance. Approach: We review new professional standards and global guidelines, then propose an architecture for adopting AI in internal auditing. Key components include AI-driven risk assessment, automated control testing, and generative AI for reporting, underpinned by robust governance controls. Technical considerations such as model explainability, data quality, and bias mitigation are addressed in depth. Findings: Properly implemented, AI can double audit efficiency and

coverage[1][2], enabling 100% transaction testing and real-time assurance. Internal audit's use of AI must however adhere to strict safeguards: our mapping of ISO 42001 and NIST's AI Risk Management Framework reveals that governance, risk assessment, and continuous monitoring are essential to maintain auditor independence and prevent ethical lapses. A pseudocode-driven case study illustrates how internal audit can evaluate an AI model's fairness and accuracy as part of an audit. Implications: This research offers internal audit departments a blueprint to become AI-enabled trusted advisors. By following IIA Standards and global AI frameworks, internal auditors in the GCC and worldwide can harness AI's power to provide deeper insights and strategic value, while upholding accountability and public trust in an era of pervasive AI.

02 Introduction

Artificial Intelligence (AI) has rapidly moved from experimental tech to a mainstream component of business operations. By 2025, AI is transforming industries and business functions across the globe, with the Gulf Cooperation Council (GCC) region at the forefront of adoption[3]. A recent survey of over 4,000 audit professionals found that AI use in internal audit is poised to surge – 39% of internal auditors were already leveraging AI tools in 2025, and adoption is expected to double to 80% by 2026[4]. This explosive growth signals a pivotal moment for the internal audit (IA) profession. Internal audit, traditionally seen as a laggard in tech adoption, now faces both an opportunity and an imperative: embrace AI to enhance assurance and insight, or risk falling behind other business functions and stakeholder expectations[5][6].

In recognition of these trends, The Institute of Internal Auditors (IIA) has modernized its professional guidance. The 2024 Global Internal Audit Standards – effective for assessments as of January 9, 2025 – emphasize strategic planning and the use of technology as critical enablers of audit quality[7]. For example, a new Standard on Technological Resources explicitly requires internal audit functions to leverage appropriate technology (which today includes AI) to perform their work effectively[8]. Likewise, Principle 9 of the new Standards urges chief audit executives to plan strategically, anticipating emerging risks and tools. These Standards reflect a consensus

that internal auditors must innovate their methodologies to keep pace with the evolving risk landscape and the data-driven, real-time decision-making environment of modern organizations.

At the same time, external frameworks around AI governance and risk management have emerged to guide organizations in responsible AI adoption. Notably, ISO/IEC 42001:2023 was introduced as the first international standard for AI Management Systems (AIMS), providing a structured approach to govern AI with trust, transparency, and accountability[9][10]. In parallel, the U.S. National Institute of Standards and Technology (NIST) released its AI Risk Management Framework (AI RMF 1.0) in 2023, built around four core functions – Map, Measure, Manage, and Govern – to help manage AI risks and ensure trustworthy AI systems[11][12]. These frameworks, though voluntary, have quickly become reference points for best practices in AI oversight. Internal audit can draw on them both when auditing their organizations' AI and when implementing AI within the audit function.

This paper presents a comprehensive exploration of how an internal audit function can become "AI-enabled" in 2025 while remaining aligned with professional standards and ethical expectations. We focus on practical steps for integrating AI across the internal audit lifecycle – from risk assessment and planning, to fieldwork testing, through to reporting and follow-up – all under a robust governance structure. We map these steps to the 2024 IIA Global Standards and to the key tenets of ISO 42001 and NIST's AI RMF, to ensure that AI use enhances audit effectiveness without compromising independence, objectivity, or stakeholders' trust. Throughout, we address challenges unique to auditing AI and using AI in audit, such as the need for auditor competence in data science, the importance of explainable AI outputs, and managing new risks introduced by AI (e.g. bias or security vulnerabilities).

The remainder of this paper is organized as follows: Section 2 provides background on the rise of AI in internal auditing and the motivation for a framework-driven approach, including regional (GCC) considerations and challenges. Section 3 reviews relevant standards and frameworks – the new IIA Standards, ISO/IEC 42001, and NIST AI RMF – and extracts principles to guide AI adoption in audit. Section 4 outlines the proposed AI-enabled internal audit methodology, detailing how AI can be used in audit planning, execution (fieldwork), and reporting, with subsections for each phase. Section 5 discusses governance and risk management controls needed to adopt AI safely,

including model validation, bias mitigation, and data governance, and illustrates an algorithmic audit procedure for an AI model. Section 6 examines potential performance gains and the results that an AI-enabled audit function can achieve, referencing early use cases and survey findings. Finally, Section 7 concludes with implications for internal audit's evolving role and future research directions, particularly for auditors in the UAE, KSA, and the broader GCC where AI is a national priority.

03 Background and Motivation

AI's Impact on Internal Auditing: In the last few years, AI has moved from concept to reality in the corporate world. Organizations now deploy AI for everything from customer service chatbots to predictive maintenance and fraud detection. The GCC region is a notable leader in this trend – by 2023, 62% of GCC companies reported using AI in at least one business function, slightly ahead of global averages[3]. Governments in the UAE and Saudi Arabia have launched national AI strategies and centers of excellence, signaling top-down support for AI innovation. For internal audit, this means two things: First, auditors must be prepared to audit AI applications within their organizations, evaluating algorithms, data integrity, and AI-driven decisions for risk and compliance. Second, internal audit functions themselves can leverage AI to improve how they conduct audits. Recent industry surveys underscore the urgency – nearly half of auditors admit that their function's use of AI lags behind other departments[5], even as audit teams face pressure to “do more with less” and provide deeper insights. AI offers internal audit the potential to analyze entire data populations, monitor processes continuously, and identify patterns that manual methods might miss. This potential to enhance assurance quality and efficiency is a key motivator for AI adoption in audit.

Challenges Driving the Need for a Framework: Embracing AI in internal audit is not without challenges. Internally, audit departments often have limited technology budgets and may lack personnel with data science skills. Culturally, there can be resistance – some auditors worry AI might replace human judgment or even their jobs. In practice, however, AI is better seen as augmenting auditors rather than replacing them[13]. AI can automate tedious tasks (like checking thousands of transactions for anomalies), freeing auditors to focus on high-value activities like investigating exceptions and advising on improvements[14][15]. Another challenge is ensuring that using AI does not compromise the core principles of internal auditing (independence, objectivity, due care). For

example, if an audit team relies on an AI tool to flag control violations, how do they know the tool is reliable and unbiased? If management is also using AI for monitoring, how does internal audit maintain a fresh, independent perspective and not just rehash what management's AI reports? These questions highlight the need for a structured framework. Without clear guidelines, there is risk of ad-hoc AI adoption that could lead to errors or ethical pitfalls – such as overreliance on AI (“automation bias”), data privacy breaches, or unintentional discrimination by AI models. A well-defined framework helps anticipate these issues and embed controls and checkpoints in the process.

Global Standards and Regional Context: The evolving regulatory and standards landscape provides further motivation to approach AI in audit systematically. The new IIA Global Internal Audit Standards (2024) were crafted in response to an environment of rapid technological change. They incorporate more guidance on technology usage and even include specific requirements for internal audit to consider technology risks and opportunities in planning engagements[7]. Topical guidance on auditing emerging risks (like AI) is expected to follow as part of the IPPF's “Topical Requirements”. Meanwhile, standards bodies and governments worldwide are acting on AI governance. ISO/IEC 42001 in late 2023 delivered a management system standard for AI, comparable to ISO 27001 for information security. It emphasizes risk management, ethical principles (like fairness and transparency), lifecycle governance, and third-party risk oversight for AI[10] [16]. Organizations that adopt ISO 42001 can seek certification to demonstrate their AI processes are under control. Internal audit will naturally be involved in assessing readiness for such certifications or auditing compliance post-implementation. Similarly, NIST's AI Risk Management Framework, though voluntary, is being referenced by regulators and industry groups as a baseline for AI risk controls[17][18]. It offers a taxonomy for thinking about AI risks (spanning from context establishment to measuring and mitigating risks, and governing AI programs). For internal auditors in regions like the UAE and KSA, aligning with these global frameworks can help ensure local AI initiatives meet international best practices and avoid insular approaches. Moreover, regulators in financial services and other sectors in the Middle East are beginning to expect robust AI governance – for instance, central banks are discussing model risk management guidelines that encompass AI models. All these factors make it clear that internal audit needs a coherent approach to auditing AI and using AI, grounded in recognized standards and adaptable to local regulatory expectations.

Internal Audit's Evolving Role and Stakeholder Expectations: The role of internal audit is expanding from purely a compliance watchdog to a strategic advisor that can anticipate risks and drive organizational improvement. This evolution is accelerated by AI. With AI enabling more proactive and comprehensive risk monitoring, internal audit has the chance to provide assurance in near real-time and to cover a broader risk spectrum (including strategic and operational risks that might have been outside traditional audit scope). For example, continuous auditing systems powered by AI could detect control breakdowns or fraud indicators as they happen, not months after the fact[19][20]. Such capabilities are highly appealing to boards and audit committees, who increasingly ask internal audit to deliver insights on emerging risks (cybersecurity, AI ethics, ESG, etc.) rather than just retrospective findings. A 2025 Deloitte survey noted that over 50% of CFOs are concerned about risks from technologies like generative AI and expect internal audit to assess those impacts[21]. In response, internal auditors are upping their game: 84% say that AI skills are important when hiring new auditors[22], and more than 45% report that training in AI tools has the greatest positive impact on increasing AI adoption in audit[22]. In summary, the motivation for this research and framework is clear. Internal audit stands at a crossroads where it must integrate AI to remain effective and relevant, but do so in a controlled, principled manner. By leveraging global standards and learning from early adopters, internal auditors can navigate this transformation successfully, ultimately strengthening their role as guardians and advisors in the age of AI.

04 **Standards and Frameworks for Trustworthy AI in Audit**

To build an AI-enabled internal audit function that is both effective and safe, we anchor our approach in three key reference points: (1) the 2024 Global Internal Audit Standards (IIA Standards), (2) ISO/IEC 42001:2023 for AI management systems, and (3) NIST's AI Risk Management Framework (AI RMF 1.0). Each offers guidance on different aspects – professional practice, organizational AI governance, and risk management respectively. Together, they form a compass to guide internal audit's AI journey. We summarize each and draw out the implications for internal audit.

2024 IIA Global Internal Audit Standards: The IIA's new Standards consolidate and update the professional requirements for internal auditors worldwide. While they are principle-based and do not prescribe specific technologies, the updated standards

clearly acknowledge the need for auditors to adapt to emerging technology. For instance, the Standards highlight the importance of strategic planning (Principle 9) and mandate that “the internal audit function must ensure it has access to the necessary tools and technology to fulfill its responsibilities” (as reflected in Standard 10.3 on Technological Resources)[8]. In practice, this means audit departments are expected to invest in tools like data analytics and AI when appropriate to increase audit quality and efficiency. The new Standards also reinforce risk-based planning and continuous risk assessment – tasks that AI can significantly enhance. Furthermore, the IIA has been proactively developing guidance on auditing AI itself. Their recent AI Auditing Framework (published in 2024) provides a foundation for auditors to understand AI risks and controls[23]. It leverages the Three Lines Model to outline roles: Governance (boards) should set oversight of AI, Management should implement and monitor AI controls, and Internal Audit provides assurance or advisory over those processes[24][25]. The IIA framework emphasizes areas like data governance, algorithm testing, security, and ethics in AI – echoing many concepts from NIST and ISO – and points auditors to resources including the NIST AI RMF as supplemental guidance[26][27]. Thus, the IIA Standards set the expectation that internal auditors will both use technology and audit technology, aligning with global best practices.

ISO/IEC 42001:2023 (AI Management System Standard): ISO 42001 is the first international standard that specifies requirements for an AI Management System (AIMS). In essence, it provides a governance framework for organizations to develop, deploy, and manage AI in a trustworthy and effective manner[9]. For internal audit, ISO 42001 is significant in two ways. First, internal auditors may be called upon to audit their organization’s compliance with this standard, either as part of internal assessments or in preparation for external certification. Second, internal audit functions should mirror some of its principles in how they govern their own AI tools. Key components of ISO 42001 include: establishing an AI governance structure with clear roles and accountability, implementing AI risk management processes (identifying, assessing, mitigating AI risks like bias or security issues), ensuring ethical AI principles are followed (e.g. fairness, transparency, human oversight)[28][29], continuous monitoring and improvement of AI systems, and stakeholder engagement and communication about AI use[16][30]. The standard advocates a Plan-Do-Check-Act (PDCA) approach: in the AI context, that means plan by defining AI objectives and risk appetite, do by deploying AI with controls, check by monitoring performance and compliance, and act by updating processes for improvement[31][32]. An internal audit function that uses AI should adopt

a similar PDCA mindset – for example, formally planning how to use AI in audits (with defined goals and risk controls), piloting and deploying AI tools, periodically checking their performance (are the AI’s findings accurate? is it operating within authorized boundaries?), and refining the approach. ISO 42001 also underscores third-party risk management: if the organization relies on third-party AI services or data, there must be oversight. Internal auditors should therefore include vendor due diligence and data supply chain checks in audits of AI. Aligning with ISO 42001 ensures that the internal audit function’s use of AI – and the organization’s AI at large – stands on a foundation of internationally recognized best practices for governance and risk management. It provides a checklist of sorts for the controls and processes that should be in place, many of which will be referenced in our framework.

NIST AI Risk Management Framework (AI RMF 1.0): NIST’s AI RMF, released in 2023, offers a voluntary but comprehensive approach to managing AI-related risks[11]. It is built around four core functions: Map – contextualize AI systems and identify risks, Measure – analyze and quantify AI risks, Manage – mitigate and govern risks, and Govern – establish overarching policies and organizational structures for AI risk management[33][12]. Each function is further broken into categories and outcomes. For example, the Map function involves understanding the AI system’s purpose, scope, and stakeholders, and mapping out potential impacts, including harms or benefits to individuals and society[34][35]. The Measure function focuses on metrics and tools to assess aspects like accuracy, bias, robustness, and security of AI systems[36]. Manage is about risk treatment – implementing controls, redundancies, incident response plans, and deciding on risk trade-offs[37][38]. Govern spans the culture, policies, and accountability structures that ensure AI risk management is sustained, addressing things like roles and responsibilities, transparency, and supply chain issues[39][40]. For an internal auditor, the AI RMF is a valuable blueprint when auditing an AI system or the organization’s AI program. It essentially provides a list of what “good” looks like: e.g., does the organization have an inventory of AI systems and their risk profiles (Map)? Are there quantitative bias and performance evaluations in place (Measure)? Are there procedures to retrain models or shut them down if they go out of bounds (Manage)? Are there governance committees or policies for AI ethics (Govern)? In our context of using AI within internal audit, the same functions can be applied. When internal audit adopts an AI tool, the audit team should Map the tool’s intended use and limitations (is it for transaction analysis? what data does it use? who could be impacted by errors?). They should Measure its performance – perhaps by testing it on known data or continuously

monitoring false positives/negatives. They must Manage the risks – for example, if the AI tool flags too many irrelevant issues (noise), they might adjust thresholds, or if it's a machine learning model that could drift, they schedule periodic retraining or validation. And they need to Govern their use of AI – assign an owner for the tool, set policies on when auditors can rely on AI output versus requiring manual verification, and ensure documentation of how the AI is integrated into audit workflow. The AI RMF's emphasis on characteristics of trustworthy AI (valid, reliable, safe, secure, explainable, accountable, and unbiased systems) aligns with internal audit's mandate to ensure reliability and integrity of processes[41][42]. By using the AI RMF as a guide, internal auditors can systematically evaluate both the AI they are auditing and the AI they are using, ensuring no dimension of risk is overlooked. Notably, the IIA's AI Auditing Framework explicitly lists the NIST AI RMF as a key resource for auditors[27], reinforcing that the profession sees value in this framework.

In summary, the 2024 IIA Standards set the expectation for technology integration and due diligence in internal audit, ISO 42001 provides a governance and quality blueprint for AI, and NIST's AI RMF offers a process to identify and manage AI risks. Our framework for AI-enabled internal auditing will draw on these, ensuring that any use of AI by internal auditors or any audit of AI within the organization meets the rigor these standards demand. We next turn to how internal audit can practically infuse AI into its activities, with these guiding principles in mind.

05 AI-Enabled Internal Audit Methodology

An AI-enabled internal audit function incorporates AI tools and techniques at each major phase of the audit lifecycle. We structure this methodology into three phases aligned with traditional audit processes: (1) Planning and Risk Assessment , (2) Fieldwork and Testing , and (3) Reporting and Follow-Up . In each phase, we will describe how AI can be deployed to enhance effectiveness and efficiency, and discuss how to do so in adherence with the standards and frameworks outlined above. Figure 1 provides an overview of how AI components integrate into the internal audit lifecycle, with governance and oversight wrapping around the entire process as a continuous safeguard.

Figure 1: AI-Enabled Internal Audit Framework. The framework depicts the internal audit cycle augmented with AI tools and a governance overlay. In the planning phase, AI-

driven analytics (such as machine learning models and natural language processing) analyze enterprise data and external information to identify high-risk areas and inform the audit plan. During fieldwork, AI applications—ranging from robotic process automation (RPA) bots to anomaly detection algorithms and computer vision for processing documents—execute audit procedures or tests in parallel with auditor oversight. The results feed into a central Fusion Engine (analogous to a multimodal fusion of insights) that compiles findings. In the reporting phase, generative AI assistants help draft findings and recommendations, while data visualization tools create dynamic dashboards. Throughout all phases, an AI governance layer (aligned to ISO 42001/NIST RMF) monitors AI performance, bias, and compliance, and an internal audit data scientist or “AI champion” reviews AI outputs. The process continuously loops, as insights from audits (and changes in risk profiles) are fed back into the risk assessment models for the next cycle, exemplifying continuous auditing.

06 **Audit Planning and Risk Assessment with AI**

Planning is foundational to internal audit, determining where to focus limited resources. Traditionally, planning relies on management interviews, manual risk assessments, and auditor judgment, which can be time-consuming and sometimes subjective. AI offers powerful tools to enhance this phase by analyzing large data sets and spotting patterns humans might miss. Under the new IIA Standards, planning must be risk-based and strategic – AI can turbocharge the “risk-based” part by providing data-driven risk insights[43].

One of the first opportunities to use AI is in the risk assessment process that drives the annual audit plan and individual engagement planning. Machine learning (ML) models can ingest historical data (e.g. past audit findings, incident reports, financial and operational data) along with external data (industry trends, economic indicators) to predict which business units or processes have the highest risk of control failures or fraud in the coming period. For example, an internal audit function can train an ML classification model to predict the likelihood of a business unit receiving a high-risk audit rating, based on attributes like change in management, complexity of operations, past issues, etc. Predictive analytics of this sort allows “dynamic risk assessment” – continuously updating the audit plan as risk factors change[44]. Deloitte reports that some IA teams are already using predictive models to identify high-risk areas in real

time, moving away from static annual risk assessments[44]. The benefit is a more responsive audit plan that can allocate resources to where emerging risks truly lie, rather than being locked into an outdated plan.

Another AI tool for planning is Natural Language Processing (NLP) . Internal auditors often gather information from unstructured sources – surveys, meeting minutes, policies, even social media – to gauge risk areas and stakeholder concerns. NLP algorithms can quickly summarize key themes from large text data. For instance, if the Chief Risk Officer collects narrative risk self-assessments from 30 department heads, an NLP model can parse these free-text responses and highlight the most cited risks or process pain points, which an auditor might otherwise take days to read through[45]. One audit team used an NLP summarizer to process lengthy survey answers from executives about emerging risks; the AI highlighted that “cybersecurity,” “third-party AI,” and “compliance training” were recurrent phrases, helping the team focus on those domains[45]. This approach aligns with the NIST AI RMF’s Map function – understanding context by processing stakeholder inputs – and ensures the audit plan is grounded in broad-based information.

AI can also support what we might call “audit intelligence gathering”. Generative AI (GenAI) like GPT-4 can assist auditors in planning an engagement in a domain they are less familiar with. For example, before auditing a complex new AI system in the organization, an auditor could use a secure GenAI assistant (preferably an internal one to maintain confidentiality) to explain technical concepts, relevant regulations, or typical controls for such a system[46][47]. This is analogous to having a virtual research assistant. The IIA Global Best Practices report notes that auditors have started using GenAI tools for tasks like drafting audit scope memos, developing initial risk and control matrices, and even formulating interview questions for clients[48][49]. For instance, an auditor might prompt an AI: “What are common controls for a machine learning model deployment process?” and use the answer as a starting reference (to be vetted with professional judgment). Such usage can save time and ensure no major area is overlooked in planning.

There are important considerations to using AI in planning. Data quality is paramount – predictions are only as good as the data fed in. Internal audit must work with management to obtain clean, relevant data (e.g., consistent loss incident data or HR records indicating organizational changes) for the ML models. Additionally, transparency

is required: if an AI model flags a particular unit as “high risk,” the chief audit executive (CAE) will need to explain to the audit committee why. This is where explainable AI techniques come in. Tools like SHAP (SHapley Additive exPlanations) can identify which factors contributed most to the model’s risk score for a given unit (e.g., “significant increase in revenue with declining headcount and control issues last year”) – information the CAE can use to justify the audit plan. In alignment with ISO 42001, before relying on an AI’s output, internal audit should perform a validation. For a predictive risk model, that might involve back-testing it against known outcomes or having auditors review a sample of its predictions for reasonableness. One approach is a hybrid model: use AI to generate a preliminary risk ranking, then have a management risk committee or auditors adjust the plan with qualitative judgment. This ensures AI augments but does not replace human oversight, consistent with the principle of human-in-the-loop and the IIA’s caution that professional judgment remains essential[50][51].

Once the audit plan is set, AI can also help with resource allocation and scheduling. RPA bots can pull data on staff availability, expertise, and previous audit schedules to suggest optimal scheduling for engagements. While this is more of an operational efficiency use case, it contributes to a smoother planning phase, freeing audit managers from manual scheduling tasks.

Overall, the planning phase illustrates some of the clearest wins for AI in internal audit: better risk focus and time saved on information gathering. A comparison between traditional and AI-enhanced planning is shown in Table 1. By leveraging AI in line with Standard 10.3 (technological resources) and the risk orientation of the new Standards, internal audit can begin each audit with a stronger fact base. However, governance must be in place – any AI-generated plan or analysis should be reviewed by experienced auditors, and the models used should be documented, tested, and updated as needed (reflecting the PDCA approach from ISO 42001). When done correctly, planning with AI positions the audit function to tackle the most significant risks and provides a strong justification for its audit priorities to stakeholders.

Table 1: Traditional vs. AI-Enhanced Audit Planning

PLANNING TASK	TRADITIONAL APPROACH	AI-ENHANCED APPROACH	BENEFIT
Annual risk assessment	Qualitative surveys and auditor judgment to rank risks.	ML model analyzes historical data and trends to predict high-risk areas[44].	Data-driven risk prioritization; dynamic updates as conditions change.
Gathering risk insights	Manual reading of reports and policies; interviews.	NLP summarizes large text collections (policies, survey responses) for key themes[45].	Broader information coverage in less time; highlights risk signals humans might miss.
Audit scoping	Auditor research on new topics; consulting frameworks.	GenAI assistant provides background on processes, regulations, and suggests scope items[46].	Faster upskilling on unfamiliar areas; more comprehensive scope documentation drafts.
Audit plan approval	Subjective rationale based on experience.	Explainable AI provides data-backed rationale (e.g. risk scores and drivers for each auditable entity).	Greater confidence for stakeholders (audit committee) in why plan targets are chosen[52].

07 Fieldwork and Testing: AI in Audit Execution

The fieldwork phase is where internal auditors “get their hands dirty,” examining processes, testing controls, and analyzing evidence. It is also the phase where AI can create the most immediate efficiency gains, by automating routine testing and expanding the scope of analysis. The goal is to enable auditors to cover more ground (potentially testing entire data populations rather than samples) and to focus their expertise on investigating anomalies and complex issues. However, using AI in fieldwork must be carefully managed to maintain audit reliability – the outputs of AI tools should be treated as evidence to be evaluated, not as oracle answers to be unthinkingly accepted.

A primary use of AI in fieldwork is in data analytics for control and transaction testing . Many internal audits involve testing large volumes of transactions for exceptions (e.g., checking if any procurement spend was split to bypass approval limits, or if any user accounts have anomalous access patterns). Traditionally, auditors would use sampling or basic data filters. AI can perform these tests more thoroughly. One example is using anomaly detection algorithms (a form of unsupervised ML) to flag unusual transactions in financial data. An anomaly detection model can establish a baseline of normal

behavior (for instance, typical ranges for transaction amounts on particular days, or typical combinations of user roles and actions in a system) and then identify outliers that deviate from the norm. Internal audit at some banks have employed such models to scan millions of transactions and have successfully identified outliers indicative of control violations or errors that were not caught by rule-based checks. Notably, AI doesn't need to replace auditor-designed tests but can complement them – auditors can feed known red-flag rules into an RPA script and simultaneously run an ML anomaly detector to catch the unknown unknowns. The result is a more comprehensive coverage[53].

AI is also enhancing continuous auditing techniques. By embedding AI monitors in systems (or having AI-powered dashboards), internal audit can effectively audit in “real-time.” For example, consider an AI system monitoring ERP logs for segregation of duties (SoD) conflicts. It can continuously parse user activity logs and cross-reference with role permissions to alert if a single user performed incompatible tasks (like creating a vendor and approving a payment). In a manual world, an auditor might test SoD quarterly by taking a sample of logs; with AI, every incident can be flagged as it happens for investigation. This moves internal audit toward a continuous assurance model, which is particularly valuable in fast-moving or high-volume environments like trading operations or large retail transaction systems. In the GCC, where many enterprises are rapidly digitizing, such continuous auditing aligns with the ambition to maintain oversight without slowing down innovation.

Another domain is automated inspection of documents and contracts . Internal audits often involve reviewing documents – policies, contracts, invoices, etc. – for compliance or accuracy. AI techniques in computer vision and NLP can assist here. For instance, an AI vision model can scan thousands of invoice images to check if critical fields (vendor name, amount, date) match across systems, flagging any discrepancies or potentially fake invoices (using anomaly detection on the formats). NLP models can read through lengthy contracts or policy documents and extract key clauses or deviations from standard templates. An internal audit of procurement contracts could deploy an NLP tool to identify any contracts missing required anti-corruption clauses, or to compare payment terms against company policy, significantly speeding up what would otherwise be a tedious manual reading exercise. This kind of AI usage was unimaginable a decade ago but is feasible today with high accuracy.

Generative AI also has a role in fieldwork, particularly in guiding auditors through complex code or configurations. For example, auditing an AI algorithm itself may require reading code. A GenAI trained on code (similar to GitHub's Copilot) could assist an auditor in understanding a piece of code, or even generating unit tests to see how that code behaves with different inputs. While this veers into IT audit territory, as more business processes rely on algorithms, internal auditors in finance or operations might find themselves auditing a Python script or a machine learning model's code. AI helpers can translate code into plain language explanations or identify potential issues in the code (like hard-coded credentials or logic bombs) for the auditor to further inspect.

The internal audit function can incorporate AI in fieldwork through a combination of in-house developed analytics, third-party audit analytics platforms, and general AI services, depending on the organization's size and resources. Big Four firms have already integrated AI into their audit software; for example, some use AI modules to analyze journal entries for dozens of risk factors simultaneously (amount, user, timing, descriptions) to flag entries for auditors to verify. Similarly, a Middle East telecom's internal audit department might use a vendor tool that applies machine learning to network access logs to find irregular access patterns indicating possible security breaches to investigate.

However, caution is warranted to ensure quality and reliability. The principle of "trust but verify" applies to AI outputs. If an AI tool flags 50 transactions as suspicious, auditors should review those items just as they would a sample picked by traditional means – perhaps even more critically, knowing AI can sometimes produce false positives or negatives. One challenge noted is that AI might flag so many exceptions that auditors can be overwhelmed. To manage this, internal audit can adjust the sensitivity of models or focus them on higher priority risks. It may also leverage the ISO 42001 concept of continuous improvement: monitor how many of the AI-flagged issues actually turn out to be real issues, and tune the model accordingly (essentially calibrating precision vs. recall). Another key control is documentation: auditors need to document not only their findings but also how the AI was used to obtain them. This includes saving the parameters or rules used by AI, logging the version of any model (since model updates could change results), and maintaining an audit trail for the AI's operations. This is crucial for transparency – both for internal validation and in case any stakeholder (e.g., external auditors or regulators) ask how an audit conclusion was reached.

Quality assurance (QA) within the audit function should incorporate reviewing the proper use of AI in fieldwork. For example, internal audit's methodology might require that if AI is used for testing, a second auditor or the audit supervisor reviews the AI output and the follow-up work done on it, to ensure nothing was taken at face value incorrectly. This parallels how one would supervise junior auditors – in fact, one can analogize AI tools to very fast but somewhat inexperienced junior auditors who can sift data but may not understand context; they need oversight from a seasoned auditor to interpret results correctly. This aligns with the IIA's guidance that AI outputs should be treated akin to an entry-level auditor's work, subject to refinement and professional judgment[50][51].

By infusing AI into fieldwork judiciously, internal audit can achieve near total coverage in certain tests and detect issues that standard sampling might miss. The AI-enabled approach also tends to reduce human error in analysis – for instance, an RPA script will not accidentally apply the wrong threshold when checking approvals (assuming the script is correctly programmed), whereas a human might slip. A survey found that 13% of auditors expect AI to increase accuracy and reduce human error in audits[2]. Table 2 gives examples of specific audit tests and how AI can enhance them. These advances do not remove the auditor from the process but change their role: instead of manually ticking and tying or hunting for anomalies, the auditor now verifies and investigates AI-identified items and spends more time on root cause analysis and discussions with management about fixes. This elevates the value of the audit. It also means auditors will need to develop some level of data literacy to effectively use these tools – a point discussed later in the context of training.

Table 2: Examples of Audit Tests Enhanced by AI in Fieldwork

AUDIT TEST AREA	TRADITIONAL METHOD	AI-ENHANCED METHOD	OUTCOME
Expense reimbursement audit	Sample 30 expense reports, check receipts manually.	Computer vision model scans all receipts (100%) for validity (e.g., matching amounts, dates) and policy compliance (flagging alcohol or weekends). NLP reads descriptions for policy keywords.	Detects policy violations across entire population; saves auditor weeks of manual review.
User access rights review	Review top 10 critical systems, compare user lists to HR termination list, sample roles for SoD conflicts.	AI agent continuously monitors all systems' access logs and HR data. ML flags any active access for terminated staff (in real time) and uses graph analytics to find toxic combinations of access permissions across systems.	Immediate identification of access control failures; comprehensive SoD coverage rather than sampling[54].
Procure-to-Pay controls	Manually verify a sample of POs for 3-way match (PO, receiving, invoice) and approvals.	RPA bot and anomaly detection model perform 3-way match on all transactions. Any mismatches or approvals outside limits are flagged. ML clusters invoice data to find unusual patterns (e.g., identical amounts repeated, or round-dollar amounts just under approval limits).	Complete assurance on transaction matching; identification of subtle fraudulent patterns (e.g., split purchases) that rules might not catch.
IT configuration compliance	Review a sample of system configuration settings against benchmarks.	Agentic AI scripts query configurations of all servers/network devices. NLP compares settings to CIS benchmark text and notes deviations; GenAI suggests potential impact of deviations.	Full inventory of misconfigurations; context on severity of each deviation to prioritize fixes.

08 Reporting and Communication: AI for Insightful Reporting

After fieldwork, internal auditors face the critical task of communicating results through audit reports, presentations, and sometimes interactive dashboards. This phase benefits from AI in two major ways: speeding up the preparation of reports (efficiency) and enhancing the clarity and customization of insights (effectiveness). The 2024 IIA Standards stress that internal audit must add value and communicate effectively – a well-crafted audit report is essential to that, and AI can assist in crafting and tailoring messages for different stakeholders.

One of the breakthrough applications of AI for reporting is using Generative AI to draft audit reports. Internal audit reports typically have a structured format and must convey sometimes complex issues in an understandable way. Generative models (like GPT-based systems fine-tuned on audit writing) can produce initial drafts of audit observations or even full reports in a fraction of the time it takes an auditor to write from scratch. For example, by feeding the AI a structured set of inputs – the condition, criteria, cause, and effect for each finding (the classic 4Cs of audit observations) – the AI can formulate a narrative that integrates these points, possibly suggesting a concise recommendation as well. A KPMG case noted by the IIA describes how an internal audit team used retrieval-augmented generation (RAG) techniques with organizational templates and style guides to produce a high-quality first draft of a report in minutes[55] [56]. The AI was provided context like the company's standard report template and previous similar reports, enabling it to output a draft closely aligned to expectations. Such a draft still requires auditor review and polishing – indeed, auditors must check for factual accuracy and tone. But it can eliminate writer's block and ensure consistency in language. It's akin to having a junior auditor prepare a draft that the audit lead can then refine.

AI can also help in customizing communications for different audiences. A challenge auditors face is translating detailed findings into language and emphasis suitable for, say, the audit committee vs. local process owners. GenAI can be used to rephrase or summarize content at different levels of detail. An auditor might prompt the AI: "Summarize this 5-paragraph detailed finding into a 2-sentence executive summary," and another prompt to "Explain this finding in technical detail focusing on what the IT operations team needs to do." The AI's ability to adjust tone and complexity can aid auditors in producing versions of the message for different stakeholders quickly. This supports better stakeholder understanding and engagement – a key aspect since an audit report's value is only realized if stakeholders read and act on it.

Another reporting aspect is visualization. AI-powered data visualization tools can automatically generate charts or even narrative explanations of data. If the audit involved analysis of, say, trends in policy compliance, an AI tool can suggest the best visualizations (bar vs. line chart) and even create them from the data, highlighting key points ("Month 5 had a spike in non-compliance"). Modern BI (business intelligence) platforms often include AI assistants that can answer questions about data ("Which department had the highest increase in issues?") and produce visuals. Internal audit can

leverage these to create more insightful reporting dashboards for management, making audit results more interactive. Especially for continuous auditing outputs, a live dashboard supplemented by AI commentary could replace or complement the static PDF report.

It is important that while AI can draft and format, the internal auditor remains the final editor. The IIA's guidance and common sense dictate that auditors must ensure accuracy and fairness of reporting[50]. GenAI might sometimes fabricate plausible-sounding text (a known issue called hallucination) or use phrasing that overstates or miscommunicates the severity of an issue. Therefore, internal audit should treat AI-generated text like a first draft from a human – useful, but needing validation. Some organizations require audit management to review 100% of AI-generated content for a period until trust is built in the tool. Over time, as the AI perhaps gets fine-tuned on an organization's specific style and prior reports, the reliance can increase, but human sign-off is non-negotiable.

From a standards perspective, using AI in reporting aligns with the efficiency goals and does not conflict with any requirements, provided the confidentiality of information is preserved (e.g., if using a cloud AI service, sensitive data must be protected or the model brought on-premise). In fact, Standard 13 ("Communicate Results") of the new IIA Standards would welcome innovative methods to enhance clarity and impact of communication. One can imagine future QA reviewers commenting positively on effective use of automated tools to expedite reporting.

A noteworthy emerging practice is the concept of an "insights engine" that continuously updates management on risk and control issues. Instead of waiting for a formal report at the end, some audit functions are experimenting with more agile communication – e.g., sending out AI-generated brief memos as soon as issues are identified and validated, possibly even through chatbots or collaboration tools. This can keep management informed in near real-time. An AI assistant, for instance, could monitor the progress of an audit in an audit management system and proactively draft interim updates: "This week, 3 new issues were identified in Procurement. Two are medium severity relating to policy compliance. No high findings so far. Testing is 60% complete." This kind of update, if accurate, can be valuable for audit leadership to know where things stand or to inform management if asked. It basically mines the audit documentation and writes a status summary. While not a replacement for conversation, it can standardize and speed up status reporting.

In summary, AI in reporting can reduce the drudgery of compiling reports and allow auditors to focus on verifying the message and formulating impactful recommendations. By using AI to tailor communication, internal audit can better meet stakeholders' needs – busy executives get concise insights, while operational managers get detailed actionable advice. The time saved in drafting can be reinvested in dialog with management about fixing issues, which is ultimately where audit's value is realized. A Wolters Kluwer survey found that freeing auditors from basic tasks (like documentation) allows them to focus on more strategic activities, which 24% of auditors anticipated as a benefit of AI adoption[2]. Reporting is a prime area where this shift can occur. The audit message still comes from the auditor's expertise, but AI acts as an enabling pen and translator, guided by the auditor's hand. With these phases covered, we have outlined how AI can be woven into the fabric of internal audit work. Next, we address how to keep that fabric strong and unfrayed – ensuring that AI is used responsibly and with proper controls, so that audit quality and ethics are never compromised.

09 **Governance, Risk Management, and Controls for Safe AI Adoption**

Incorporating AI into internal audit brings not only opportunities but also new risks. Just as internal auditors insist that management put controls around any new technology, the audit function must practice what it preaches by establishing governance and controls for its own use of AI. Moreover, when auditing AI-driven processes in the organization, auditors need a structured approach to evaluate those systems. In this section, we outline the governance and risk management practices that enable safe AI adoption in internal audit, consistent with ISO 42001 and NIST AI RMF principles. We also present a high-level algorithm (pseudocode) that internal audit can follow when auditing an AI system, illustrating how these practices come together.

AI Governance within Internal Audit: The internal audit function should define clear governance for any AI tools it uses. This starts with assigning responsibility. Many organizations have formed AI governance committees or working groups; internal audit should either be represented in those or form its own steering committee for audit technology. For example, an internal audit department might designate an "AI Champion" or appoint the head of audit methodology to oversee AI tool adoption, ensuring alignment with audit methodology and standards. This person or group would approve

what AI tools are used, review their performance periodically, and ensure auditors are trained. They would also interface with IT and data security to ensure AI tools comply with data privacy and security policies. The NIST RMF Govern function calls for defined accountability and processes for AI risk management[57][58] – applied internally, this means having policies on AI usage in audit. A policy might state, for instance, that “Any AI tool used in audit must be validated on a sample data set with known outcomes before use on live audits, with results documented” and “Auditors must not input confidential data into external AI platforms without approval and proper agreements in place” (to prevent data leakage). The internal audit charter could even be updated to reflect a commitment to use innovative techniques (like AI) responsibly to fulfill audit’s mission.

Risk Assessment of AI Tools: Before deploying an AI tool, internal audit should perform a risk assessment of that tool – essentially, audit your AI before you trust it. ISO 42001 emphasizes an impact assessment for AI systems[10]. If internal audit plans to use an AI model to identify risky transactions, some questions to assess: How complex is the model (simple decision tree vs. black-box neural network)? What’s the risk of false negatives (missing a key issue)? Is the data it uses sensitive (client personal data, etc.) that needs special handling? What bias could be present (is the model less effective in certain business units due to less data)? What’s the vendor risk (if it’s third-party software, is the vendor reputable and secure)? This assessment identifies needed controls. For example, if bias is a concern, a control could be to test the model outputs across different subgroups of data to ensure fairness. If data sensitivity is an issue, perhaps the AI processing is done on-premises or on anonymized data. If the model is black-box, maybe require an explainability tool or limit usage to advisory (not assurance) purposes until more confidence is gained.

Technical Controls and Validation: Internal audit should implement controls to maintain the integrity of AI outputs. Key among these is validation. Just as models in finance (like credit risk models) undergo periodic validation by independent parties, internal audit’s AI models should be validated – likely by someone within the audit team with analytics expertise or by co-sourcing with a data science team. Validation could include checking that the model meets its intended purpose, testing it on historical cases (did it flag past known issues?), and verifying stability (if a slight change in input causes a wild change in output, that’s a red flag indicating overfitting or instability). Another control is change management: version control for AI models and RPA scripts should be in place, so any

updates are tracked and tested. This ensures that if a model is updated mid-year, one can compare results before and after, and roll back if needed, akin to how audit documentation tools are managed under change control.

Bias and Ethics: AI can inadvertently incorporate bias, which is a critical risk since internal audit must be objective and fair. For instance, if an audit planning model were fed mostly financial data, it might under-prioritize risks in softer areas like compliance or culture. Recognizing this, internal audit should consciously incorporate diverse risk factors and possibly apply fairness constraints in models (ensuring no key risk category is systematically ignored). When auditing an AI system in the business, checking for bias and fairness is part of the assurance job – for example, if auditing a HR hiring AI, internal audit should evaluate if that AI has adverse impact on certain demographics. Techniques like disparate impact analysis (comparing outcomes across groups) and counterfactual testing (would a small change in input like ethnicity change the output?) can be part of the audit program[59][60]. Moreover, internal audit should champion ethical AI use by example: any AI it uses should comply with organizational AI ethics guidelines (if they exist) or generally accepted principles like the IIA's Code of Ethics (e.g., integrity, which would mean not using AI to deceive or manipulate).

Security and Data Privacy: Using AI often means processing large datasets. Internal audit must ensure that its use of data for AI complies with data privacy laws and corporate policies. If audit pulls data from systems into an AI tool, that data should be as limited as necessary (data minimization principle) and protected. If using cloud-based AI services, encryption and agreements must be in place. Also, any outputs (which might contain sensitive info, like flagged suspicious transactions involving individuals' data) need to be handled securely. Cybersecurity is another aspect – AI tools themselves could introduce vulnerabilities (an RPA bot with access credentials, for instance). Audit should work with IT to include any AI software in vulnerability management routines. In essence, treat the AI tool as you would a new IT system going live, with threat modeling and security testing. The stakes are high: a breach or error in an audit AI tool could not only compromise data but also damage audit's credibility.

Collaboration with Second Line and IT: Internal audit should not operate in a vacuum when adopting AI. Coordination with the second line (risk management) is beneficial. Many organizations' risk functions are also exploring AI for risk monitoring. By collaborating, audit can share knowledge, possibly use common platforms, and ensure

that there's no duplication or, worse, conflicting AI assessments. Additionally, if the organization has a model risk management framework (often overseen by a risk function or a model risk committee), internal audit should comply with those policies for its own models. For example, if corporate policy requires all AI models to be registered in an inventory with documentation of their purpose and validation, audit should do the same for its models. This not only sets a good example but also provides an independent check on audit's tools.

Finally, we consolidate many of these governance practices into a simplified pseudocode algorithm below, demonstrating how an internal auditor might systematically audit an AI system (e.g., an AI used in hiring or credit decisions). This procedure reflects steps aligned with NIST's Map-Measure-Manage-Govern framework and ISO 42001 controls. It shows the auditor identifying context, examining governance, testing the model, and evaluating outcomes and controls. While simplified, it illustrates the logical flow an audit might follow, ensuring a thorough evaluation.

```
# Pseudocode: Internal Audit Procedure for Auditing an AI System function
auditAISystem(AI_System): # 1. Map: Understand context and governance of the AI
system gather_system_purpose = AI_System.getDocumentation("purpose")
gather_stakeholders = AI_System.listStakeholders() if not
AI_System.hasGovernanceCommittee: issue_log.add("No governance committee
overseeing AI system") if "ethics policy" not in AI_System.policies: issue_log.add("No
documented AI ethics principles") # 2. Map: Identify and categorize risks risks =
AI_System.getRiskRegister() # e.g., bias risk, security risk, etc. for risk in risks: if not
risk.mitigation_plan: issue_log.add("Risk '"+risk.name+"' has no mitigation plan") #
Ensure context covers societal impact if applicable if AI_System.impactAssessment is
None: issue_log.add("No impact assessment (e.g., privacy, bias) conducted for AI
system") # 3. Measure: Test technical effectiveness and fairness of AI model model =
AI_System.getModel() test_data = AI_System.getHistoricalData(withOutcomes=True)
results = model.run(test_data.inputs) performance = evaluate_performance(results,
test_data.expected_outcomes) if performance.accuracy < acceptable_threshold:
issue_log.add("Model accuracy below threshold: "+performance.accuracy) bias_metrics
= compute_fairness(results, test_data.labels) # e.g., outcomes by gender for metric,
value in bias_metrics.items(): if value > bias_tolerance[metric]: issue_log.add(f"Potential
bias detected in model output for {metric}: {value}") # Security testing if not
AI_System.hasSecurityControls("model_integrity"): issue_log.add("No integrity
```

```

protection (e.g., hash) on AI moexamdel files") attack_results =
perform_adversarial_test(model, test_data.sample) if attack_results.success:
issue_log.add("Model vulnerable to adversarial inputs (e.g., can be fooled by slight
perturbation)") # 4. Manage: Evaluate monitoring and incident response if not
AI_System.monitoring.enabled: issue_log.add("No ongoing monitoring of AI outputs in
production for anomalies") else: if AI_System.monitoring.alerts_not_reviewed:
issue_log.add("Monitoring alerts are not reviewed by management") if not
AI_System.hasRetrainingPlan: issue_log.add("No plan to periodically retrain/update
model for new data") if AI_System.getContingencyPlan() is None: issue_log.add("No
contingency plan if AI system fails or produces harmful output") # 5. Conclude and
report for issue in issue_log: record_issue(issue) summary =
generateAuditReport(issue_log, AI_System.name) return summary, issue_log

```

This pseudocode outlines an approach where the auditor first examines governance (policies, oversight), then identifies risks and checks that management has mitigations (aligning to ISO 42001's requirements for risk management and stakeholder involvement[28][57]). Then it dives into technical testing of the AI (accuracy, bias, security – covering NIST's Measure function outcomes like performance and security assessments[36][59]). Next, it checks Manage function items: monitoring, retraining, incident response[38][61]. Finally, it compiles issues for reporting, which the auditor would then discuss with management and include in the audit report. In a real scenario, each of those steps could be quite involved, and auditors may use specialized tools (e.g., bias testing software) to assist. But importantly, this framework ensures no aspect is forgotten – not just the model itself, but also the surrounding process and controls are audited.

Training and Competence: A word is due on the human factor – none of these controls or audits can happen without auditors being trained. The new IIA Standards implicitly require that internal auditors collectively have the skills needed for their plan (Principle 10 on Competency and Resources). This means CAEs need to invest in training their staff on data analytics, AI basics, and relevant tools. The Wolters Kluwer survey found 45% of auditors saw training in AI as the key to adoption[22]. Many audit groups in the GCC and globally are now including data science modules in their continuous education, hiring data analysts into audit, or partnering with external experts. The control framework should thus also include a talent development aspect: ensuring the audit team can

effectively use and scrutinize AI. Without skilled people, even the best AI governance process will falter.

“Trust but Verify” Culture: Ultimately, instilling the right culture in the audit team is perhaps the strongest control. Auditors should treat AI as a tool that can err, just as humans can. A healthy skepticism – neither unwarranted trust in AI nor irrational fear of it – should be cultivated. Internal audit leadership should communicate that using AI is encouraged to enhance work, but every conclusion must still be backed by evidence and logic that an auditor can explain. If an AI flags an issue, the auditor’s job is to investigate and validate it before reporting. If AI provides an answer, the auditor should question it, just like they would question an auditee’s explanation, until satisfied. By blending AI into the audit methodology with solid governance and a persistent emphasis on auditor judgment, the internal audit function can reap AI’s benefits while upholding its professional standards and responsibility to provide reliable assurance.

10 Performance Evaluation and Impact

To justify the integration of AI into internal audit, it is important to evaluate its performance: both in terms of the audit function’s efficiency and effectiveness and the quality of outcomes delivered. Since many audit functions in 2025 are in early stages of AI adoption, quantitative data is still emerging. However, surveys, pilot project results, and logical analysis provide strong indications of the gains AI-enabled auditing can achieve. We also consider the potential challenges observed during implementation that could affect performance (e.g., initial false positives, learning curves) and how our adaptive framework addresses them.

Efficiency Gains: The most immediate performance impact of AI is on efficiency metrics – audit cycle time, coverage, and cost per audit. As noted earlier, AI can dramatically reduce the time spent on labor-intensive tasks like data processing, document review, and report drafting. A Wolters Kluwer study found over half of internal auditors expected AI to drive productivity gains, with many eyeing cycle time reductions in the next year[1] [2]. Some anecdotal results: a pilot at a financial institution’s internal audit team using an AI tool to analyze expenses saw the fieldwork time drop by 30%, as the tool instantly flagged exceptions that would have taken auditors days to find by manual sampling. Another example comes from KPMG’s experience: using GenAI for report writing cut down report drafting from multiple days to a few hours for a first draft[55]. These

efficiency gains mean that auditors can either complete audits faster or handle more audits with the same resources.

To quantify, suppose an average audit used to take 4 weeks of effort; with AI assistance in planning, testing, and reporting, perhaps a week's worth of effort is saved – a 25% efficiency gain. In monetary terms, if an audit department's annual budget is \$X and they achieve a 20% productivity improvement, that's like getting 1.2X output for X cost. Early adopter surveys reflect such optimism: 54% of auditors in one survey believed AI would significantly improve efficiency within a year[2]. Our proposed approach targets these efficiencies by attacking known time-sinks in the audit workflow. Moreover, by aligning tasks to AI's strengths (speed, pattern recognition) and auditors' strengths (judgment, communication), we minimize wasted effort (e.g., auditors doing brute-force checks that a machine could do faster).

Effectiveness and Coverage: Efficiency is only valuable if effectiveness is maintained or enhanced. A key question: Does AI-enabled audit find more relevant issues and provide better assurance? The evidence so far is encouraging. AI enables 100% testing of certain controls, turning what used to be inferred from samples into directly observed fact. One internal audit group reported that after deploying an AI transaction monitoring tool, the number of findings in their audits initially increased – not because controls had worsened, but because they were now catching issues that were previously skating under the radar. Over time, as management fixed those and the control environment improved, findings count stabilized, but those early wins were critical in preventing potential bigger problems. Continuous monitoring by AI can also catch issues sooner, reducing the impact of control failures (e.g., detecting a segregation of duties conflict early before it leads to fraud). These improvements tie back to internal audit's mission of enhancing and protecting organizational value.

Quality is a paramount part of effectiveness. There were concerns that AI might generate false findings that waste time. In pilots, indeed auditors faced an initial surge of false positives from AI anomaly detectors not tuned properly, which could hurt productivity. Our framework's adaptive approach – adjusting models and thresholds, focusing on high-impact anomalies – is aimed at controlling this. One measure of effectiveness is the "precision" of findings: the proportion of AI-flagged issues that turned out to be real issues. Through iterative tuning, an audit team improved one model's precision from about 50% in the first run to 85% in subsequent runs, meaning

far fewer false alarms. When integrated properly, AI's false positive rate can be managed to be on par with or better than traditional methods (after all, manual audits also can pursue what turn out to be non-issues).

Another effectiveness aspect is stakeholder satisfaction. A transformed, AI-empowered audit function can deliver reports faster and often with deeper insight (like data visualizations or benchmarks) than before. This tends to increase the satisfaction of audit clients and the audit committee. Charles King of KPMG suggests aiming for measurable goals such as "raising audit client satisfaction ratings by a full point" or "reducing time from kickoff to report by four weeks" as yardsticks for transformation[62]. These are ambitious but increasingly realistic with AI. In practice, one can look at stakeholder feedback surveys before and after AI adoption. In a Middle East government entity's internal audit department that adopted process mining (an AI technique) to audit procurement, feedback from the auditee was positive – they appreciated the factual, data-backed findings and the reduction in disruption (since auditors asked for far fewer documents, having already extracted most data digitally). The audit committee also noted that the insights were more compelling, often showing trend analyses and root cause analytics that previously weren't available.

Case Example – UAE Financial Institution: As a hypothetical composite example (drawing on common experiences in the region), consider a UAE bank's internal audit function implementing our AI-enabled approach. In the first year, they integrate an AI analytics platform for continuous transaction auditing and a GenAI tool for reporting. They report the following outcomes: The audit plan became more flexible, adding two new high-risk audits mid-year that were identified by the AI risk assessment as needing attention (something they likely would have missed in a static plan). They covered 100% of payments in an AML (anti-money laundering) audit using AI, discovering 3 suspicious transactions that led to investigations – previously, their sample-based audit had given clean results and those would have been undetected. The average audit engagement time dropped from 6 weeks to 5 weeks, allowing them to perform 5 more audits than last year. On the downside, they initially struggled with too many alerts (the AML model flagged hundreds of transactions, of which only a handful were significant). They addressed this by involving their data science team to refine the scenario logic and by focusing on the top 10 exceptions at a time (risk-ranking the AI outputs). By year-end, management feedback was that audit reports were more data-driven and convincing; one executive said, "The audit findings were hard to dispute because they showed us

the full picture, not just a few examples.” The audit committee noted improved timeliness in issue reporting. These qualitative and quantitative results demonstrate the net positive impact, while also highlighting the learning curve.

Challenges and Mitigation: The performance evaluation would be incomplete without noting challenges faced and how they were overcome. Common challenges include: resistance from some auditors who were comfortable with traditional methods, initial technical glitches or inaccuracies in AI outputs, and integration issues with existing audit management systems. Change management is crucial. In our framework, we involve auditors from the start (especially in planning how AI will be used) to get buy-in, and provide training to build confidence. One GCC audit director mentioned that once auditors saw AI handling tedious tasks and not “stealing” the judgment-intensive parts of their job, their anxiety eased and they became advocates for the tools. That cultural shift is an important performance indicator too – the internal audit team’s morale and readiness to innovate can be boosted by successful AI adoption, making the function more agile for future challenges.

We should also consider external benchmarks. External quality assessments (EQA) of internal audit now increasingly ask about use of data analytics and technology. An audit function effectively using AI might score higher on the “use of technology” criteria of an EQA, reflecting positively on its maturity. If the internal audit function aspires to be “leading practice,” appropriate AI adoption is practically becoming a must-have.

In terms of risk, we assess that the risks of using AI (like erroneous results or model bias) can be kept within acceptable ranges through the controls discussed earlier. In fact, a properly governed AI may pose less risk than a poorly supervised human process, because AI can be systematically tested and improved, whereas human inconsistency is harder to detect. That said, it remains critical to monitor outcomes: metrics like “number of significant findings missed by AI that were later found by other means” or “errors in reports due to AI” should be tracked. In our approach, we recommend a post-audit review focusing on AI performance – essentially treating the AI as part of the audit team whose work gets reviewed. If any issue slipped past because an AI tool failed, that is analyzed and the tool corrected. So far, no catastrophic misses have been reported by early adopters; on the contrary, more instances are reported of AI catching what humans missed (especially in data-heavy tasks).

In conclusion, the performance improvements from integrating AI into internal audit are substantial in both quantitative and qualitative terms. When aligned with professional standards and managed prudently, AI helps internal audit do a better job faster. It is transforming audit from a periodic, sample-based, hindsight-focused endeavor into a more continuous, comprehensive, and forward-looking assurance and advisory function. This lays the groundwork for the ultimate goal: not just finding problems, but helping prevent them and guiding the organization's governance in the age of digital transformation. We now move to conclude our paper with final thoughts on the journey ahead for internal audit in leveraging AI and the future research or actions needed.

11 Conclusion and Future Outlook

The advent of AI in the mid-2020s represents a watershed moment for the internal audit profession. This paper has explored how an internal audit function can embrace AI as an enabler, not a disruptor, by adhering to new IIA Standards and aligning with robust frameworks like ISO/IEC 42001 and NIST's AI RMF. The research and framework presented demonstrate that internal audit can substantially enhance its value proposition through AI – increasing audit coverage, depth of insight, and timeliness – while still upholding the core principles of independence, objectivity, and rigor that stakeholders expect. By carefully integrating AI into planning, fieldwork, and reporting, supported by strong governance and risk management controls, internal audit can achieve what once seemed an impossible trifecta: doing more, faster, without sacrificing quality or trust.

For internal auditors in the GCC region and beyond, the message is clear: AI is not a luxury or a passing trend, but a strategic imperative. In nations like the UAE and Saudi Arabia where governments are pushing an AI and digital transformation agenda, internal audit departments are expected to keep pace to remain relevant partners. The new Global Internal Audit Standards effective 2025 reinforce this by embedding expectations around technology use and strategic foresight. An AI-enabled internal audit function is better equipped to audit the complex, AI-driven processes organizations are adopting – you cannot effectively audit tomorrow's business with yesterday's tools. Moreover, as highlighted by the IIA in its comment to policymakers, internal audit can be the front line of assurance for AI within organizations[63][64]. Rather than external regulators directly auditing AI algorithms, internal auditors – with their unique organizational knowledge and independent role – are well positioned to evaluate and assure AI systems'

trustworthiness. But to do so credibly, they must have the know-how and tools that match the task.

The journey to an AI-empowered audit function is not without challenges, but these can be addressed with a thoughtful approach. Key success factors include:

- Leadership vision and tone at the top: CAEs need to set a vision for innovation and ensure the audit committee supports the prudent use of AI. This might involve investing in technology and new skill sets, and articulating how AI will help audit deliver on strategic objectives. A clear message that “AI will augment, not replace, auditors” helps gain team buy-in[13].
- Talent and training: The audit team must be upskilled to use and interpret AI. This may involve hiring data analysts into audit teams or training existing staff in analytics, coding, and AI fundamentals. Professional certifications and training programs are emerging (e.g., the IIA’s AI auditing courses); leveraging these will accelerate competence development.
- Phase-wise implementation: A phased approach – pilot AI in a few audits, learn and refine – is advisable. Quick wins (like using GenAI for memos or RPA for evidence gathering) can build momentum. More complex implementations (like a full predictive risk model) can follow once foundational data issues are sorted and confidence is built. Essentially, crawl-walk-run: perhaps start with supervised learning tools that are easier to explain, then venture into more complex ML as trust grows.
- Continuous improvement and adaptation: AI tools and models will evolve, as will the organization’s processes and risks. The framework we proposed emphasizes feedback loops: monitor AI performance, solicit feedback from auditors and management, and adjust. Internal audit should remain agile – for instance, updating the AI risk model annually to reflect new risk factors, or incorporating new data sources (like emerging ESG metrics) as they become relevant.
- Collaboration and knowledge sharing: Internally, collaborate with IT, risk management, and data science units. Externally, internal audit can engage in forums or peer networks (e.g., IIA chapters in UAE and KSA, or global working groups) to share experiences and tools. Given that AI in audit is still maturing, auditors can

benefit from each other's lessons learned to avoid reinventing the wheel and to establish industry benchmarks.

Looking to the future, one can envision a fully “digital internal audit” function by the end of this decade. In such a vision, repetitive audit testing is largely automated, audits are triggered by intelligent monitoring systems when risk thresholds are breached, and internal auditors focus on high-level analysis, consulting on risk mitigation, and validating AI systems. Audit reports might become continuous updates via dashboards rather than periodic static documents. The skill set of internal auditors will likely further shift toward data science, systems thinking, and understanding AI ethics and regulations (especially as laws like the EU AI Act come into effect, which might mandate algorithmic transparency and audits in certain cases). Internal audit might also expand its purview to provide assurance over things like data governance and AI ethics board functioning, given its enterprise-wide view.

In the context of the GCC, with initiatives like Saudi Arabia's NEOM and UAE's drive for smart government, internal audit has an opportunity to position itself as a leader in responsible AI adoption. Auditors in the region can leverage the strong support for innovation by demonstrating that they can both use these technologies and keep them in check. Being early adopters of AI in internal audit could also elevate the function's status – showing that it is forward-thinking and business-aligned. It could open new career paths for tech-savvy auditors and attract talent who are excited about using cutting-edge tools in a traditionally conservative field.

Future research could delve into developing standardized audit programs for different types of AI (e.g., auditing a machine learning model vs. an RPA bot vs. a rules-based expert system) or case studies quantifying ROI of audit technology investments. Metrics for audit effectiveness in the AI era also merit exploration – for example, developing an “audit value index” that captures not just cost savings but risk reduction achieved through continuous auditing.

In conclusion, as organizations navigate the uncharted waters of AI, the internal audit function can serve as both a compass and anchor – guiding prudent innovation while anchoring decisions in risk management and control principles. By building an AI-enabled internal audit function under the umbrella of the new IIA Standards and informed by frameworks like ISO 42001 and NIST RMF, organizations equip themselves with a

robust mechanism to ensure AI is adopted responsibly and effectively. The synergy of human judgment and artificial intelligence promises an exciting future for internal auditing, one where auditors are not replaced by machines, but rather elevated by them to provide even greater assurance and advisory impact. With preparation and the right frameworks, internal audit can confidently audit AI, use AI, and ultimately audit with AI – securing its role as a key player in the governance of the intelligent, automated world that lies ahead.

12 References

J. Bramwell, " AI Adoption by Internal Auditors Set to Double by 2026, Survey Finds ," CPA Practice Advisor

- , May 7, 2025[4][1].
- The Institute of Internal Auditors, " Artificial Intelligence Auditing Framework ," The IIA, 2024[65][23].
- R. P. Grubenmann, " ISO/IEC 42001: a new standard for AI governance ," KPMG Switzerland, 2023[9][28].
- NIST, " Artificial Intelligence Risk Management Framework (AI RMF 1.0) ," National Institute of Standards and Technology, 2023[11][12].

Deloitte Middle East, " Reimagining the DNA of Internal Audit: The journey to revolutionize the IA function ," Middle East Point of View

- , Spring 2025[44][13].
- C. King, " Transforming Audit Through AI ," Global Best Practices, The IIA, 2025[45][63].
- R. Sounderrajan, " Integrated AI in Internal Audits ," MCA Gulf (Insights), May 2025[66][67].
- The Institute of Internal Auditors, " Global Internal Audit Standards (2024) ," The IIA, 2023[8][7].
- Consultancy-Me / McKinsey & Co., " Further adoption of AI can add \$150 billion to GCC economies ," Aug. 23, 2023[68][3].