



The Future of Internal Audit with AI

Evolving at the right pace

Governance, Risk & Compliance Services (GRCS)
KPMG Netherlands

KPMG. Make The Difference.



Table of Contents

01	Why AI matters for Internal Audit	4
-----------	-----------------------------------	---

02	Understanding AI in the Internal Audit context	6
-----------	--	---

03	How AI supports each phase of the Internal Audit lifecycle	10
-----------	--	----

04	Risks, limitations & governance of AI in Internal Audit	14
-----------	---	----

05	Required Capabilities	17
-----------	-----------------------	----

06	KPMG perspective & closing	18
-----------	----------------------------	----

Key terminology	20
-----------------	----

Contact	21
---------	----

Foreword & Executive Context

For decades, Internal Audit (IA) has played a critical role in providing independent assurance and advice over risks and controls. However, the environment in which IA operates is changing rapidly. Organisations face increasing complexity, tighter regulatory expectations, and accelerating technological developments, including the growing use of Artificial Intelligence (AI). Together, these changes challenge traditional IA approaches and raise an important question for many audit leaders: how can Internal Audit remain relevant and deliver value in this evolving context?

From our perspective, we do not see this challenge as a future consideration, but an immediate reality. Across sectors, Internal Audit Functions (IAFs) are expected to provide sharper insights, stronger alignment with organisational priorities, and greater agility. At the same time, IA should maintain independence, quality, and professional standards. Meanwhile, AI has become increasingly normalised in business processes and decision-making, creating new risks to be assessed and new opportunities to enhance IA execution. Meeting these expectations requires deliberate evolution rather than radical reinvention.

Our view is clear. The future relevance of IA will be shaped by its ability to combine strong foundational practices with modern ways of working, including the thoughtful and responsible use of AI. This does not require IA to turn into a technological function, nor does it imply innovating for the sake of innovation.

Instead, it is about equipping IA teams to operate effectively and efficiently in dynamic and evolving environments. Simultaneously, IA teams should ensure that transparency, accountability and sound professional judgement remain central to how conclusions are formed.

We support IAF in making well-governed choices about how AI and other technologies are implemented and applied within the audit function, and how AI can be audited across the organisation. In practice, this means focusing on concrete use cases, embedding appropriate governance, and aligning change with professional standards and stakeholder expectations, to ensure that trust from boards, audit committees and regulators is reinforced rather than compromised.

This whitepaper is written for Chief Audit Executives and Internal Audit leaders who seek to navigate the balance of AI implementation and thoughtful governance. It provides a clear and practical perspective on how IAFs can evolve at the right pace, using AI as an enabler, while continuing to deliver quality and value to their organisation.



Huck Chuah

Partner, Governance, Risk & Compliance Services
KPMG Netherlands



01 Why AI matters for Internal Audit

The changing risk & advisory landscape

As technology advances rapidly and artificial intelligence (AI) becomes embedded in core processes, a fundamental question is emerging: how does Internal Audit (IA) remain relevant in a world where parts of its traditional work are increasingly being automated? Technological developments and digital transformation mean that risks emerge faster and evolve more dynamically than before. In this context, it is essential that IAF continues to develop alongside these changes to remain relevant and deliver meaningful value to the organisation. To do so effectively, the function must align its ways of working, skills, and use of technology ensuring that it continues to deliver tangible value.

Regulatory expectations

Regulators and supervisory bodies increasingly expect organisations to demonstrate control over advanced technologies, including automated decision-making systems and AI-driven processes. In the European context in particular, organisations must also be able to demonstrate compliance with the EU AI Act, which introduces explicit obligations around risk classification, documentation, human oversight, and governance for high risk AI-driven systems raising the bar for IA's role in assessing and evidencing compliance in practice. Expectations around model risk management, explainability, data governance, and ethical use of technology are becoming more explicit. For IA, this translates into higher expectations regarding the depth and credibility of assurance over complex systems. Stakeholders are no longer satisfied with high-level

descriptions of controls; they expect evidence-based insights into how risks are identified, monitored, and mitigated in practice.

AI: from trend to audit necessity

AI has moved beyond experimentation and isolated use cases, while at the same time organisations are on a journey to implement AI across different processes. This shift has direct implications for all three lines of defence, particularly for IA.

AI adoption in the first and second line

In the first line, AI is used to optimise operations, support decision making, process execution, and customer interactions, often becoming an integral part of how business processes function rather than a standalone analytical tool.

In the second line, AI is used to support risk identification, draft controls and identify gaps in control frameworks, monitoring activities, and regulatory compliance. Instead of replacing oversight, these applications reshape how risks are identified, assessed, and managed on. As a result, significant parts of the organisation's risk management activities are now already supported or driven by AI driven systems.



Implications for the third line

As AI becomes embedded in core business processes, IA must be able to assess transparency, control, and accountability within these systems in a timely and scalable manner. Professional judgement remains essential within IA. However, to remain relevant and add value, the function can no longer rely solely on traditional ways of working. IA needs to use AI where it helps auditors perform their work more effectively, while at the same time expanding its assurance activities to include AI driven processes within the organisation. Established audit principles remain valid, but they need to be applied differently to ensure IA continues to add value in an AI driven environment.

For Internal Audit, the rise of AI presents both a challenge and an opportunity that goes beyond traditional assurance and advice. While the ability to provide assurance over

AI-enabled processes and controls across the organisation remains essential, AI also acts as a catalyst for the broader evolution of the Internal Audit Function (IAF) itself. Stakeholders increasingly expect IA not only to assess emerging technologies, but to operate with comparable levels of efficiency, adaptability, and digital maturity.

An IAF that continues to rely primarily on manual, fragmented ways of working risks being perceived as reactive or misaligned with how the business operates. This expectation extends beyond analytical techniques and risk identification and touches all core audit activities, including planning, preliminary investigation, fieldwork, reporting, evaluation and follow-up. Used responsibly, AI can support more consistent and timely audit planning, streamline repetitive administrative and documentation tasks, enhance audit quality through structured workflows, and improve communication and insight generation for stakeholders. By reducing the time spent on routine and

repetitive tasks, AI enables internal auditors to focus on professional judgement, critical thinking, collaboration, and delivering value. Consequently, AI is not only an audit object, but a key enabler of Internal Audit's effectiveness, relevance, and continuous improvement as the third line.

From innovation to expectation

As AI is broadly implemented in many organisations, it is also reshaping what is expected from IA. Practices that were once explored as pilots or positioned as 'innovative' are now moving closer to the mainstream. For many stakeholders, the use of AI is no longer a nice-to-have, but a sign that the function is keeping pace with the business it supports. As a result, the question is no longer whether AI has a place in IA, but how it can be adopted responsibly to support the audit function.



02 Understanding AI in the Internal Audit context

Understanding AI capabilities and constraints

AI is increasingly embedded in the tools, data flows, and decision-support processes that IA relies on. Yet the term 'Artificial Intelligence' is often used inconsistently. For internal auditors, clarity matters: knowing how AI works, what its limitations are, and where human judgement remains essential is necessary to use AI responsibly and to evaluate its outcomes with professional scepticism.

AI refers to a set of computational techniques that enable systems to recognise patterns, interpret language, learn from data, or support decisions in ways that go beyond predefined rules. In practice, this includes statistical and machine learning models that surface anomalies across large populations and forecast outcomes or classify events. Furthermore, AI includes generative models that summarise or draft new content such as text, analyses, process descriptions, or code, and it entails AI agents that can execute tasks with varying degrees of autonomy. While these capabilities can significantly expand audit coverage and efficiency, they also introduce new limitations, dependencies, and risks that IA must understand and manage.

A key distinction is that AI does not replace professional judgement. AI systems excel at processing scale, identifying correlations, and structuring large volumes of information, but they do not possess contextual awareness, ethical reasoning, or accountability. They operate based on data, model assumptions, and design choices that must be critically assessed. This makes professional scepticism more important than ever before.

Internal auditors must be able to evaluate whether AI outputs are reliable, whether underlying data is complete and appropriate, and whether conclusions drawn from AI assisted analyses are proportionate and justified. In this sense, AI reshapes how audit work is performed, but not the auditor's responsibility for conclusions, opinions, advice and assurance.

Understanding AI is about enabling auditors to ask the right questions: where is AI used, for what purpose, with what level of autonomy, and under which governance and controls. It is also about recognising where human oversight remains essential, particularly when AI influences high-impact decisions, sensitive data, or regulatory outcomes. By establishing a clear and shared understanding of AI concepts, capabilities, and limitations, IA is better equipped to use AI responsibly within its own activities and to provide credible assurance and advice on AI used elsewhere in the organisation.

How AI differs from automation and traditional analytics

While automation replaces repetitive steps with predefined rules, AI introduces adaptivity and interpretation. Adaptivity refers to AI's ability to adjust as circumstances change, for example, learning from new data, recognising evolving patterns, or refining outputs as processes, behaviours, or risks shift over time. Interpretation goes a step further by enabling AI to make sense of complex or unstructured information, such as identifying themes, relationships, or anomalies that are not explicitly defined in advance.

Where traditional analytics answer predefined questions based on fixed models, AI can help surface the questions auditors should ask in the first place by highlighting unexpected signals or areas of interest. This distinction is essential as IA functions modernise their methodologies: adopting AI is less about adding another tool and more about augmenting audit thinking, risk sensing, and evidence collection.



"The key is not how advanced the technology is, but whether you choose the right level of autonomy for the right task and remain willing to take responsibility for the outcome."

Huck Chuah

AI types most relevant to Internal Audit

AI refers to a collection of computational techniques that mimic elements of human cognition, such as language understanding, pattern recognition, and automated decision-making. In Internal Audit, the most relevant categories include Machine Learning, Deep Learning, Generative AI (GenAI) and Agentic AI (see figure 1).

Across these categories, AI amplifies auditors' reach. However, it does not yet replicate professional judgement, contextual reasoning, or ethical responsibility. These remain non-delegable roles of the auditor.

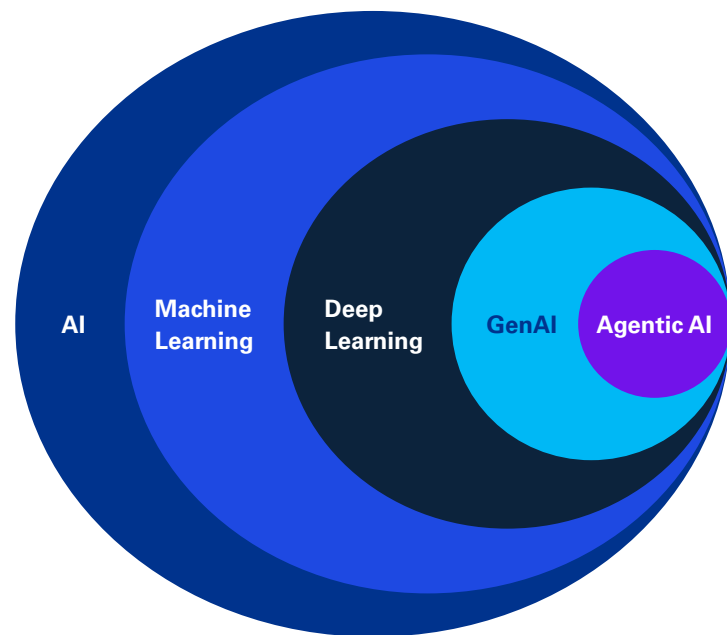
Understanding AI agents and levels of autonomy

To navigate the expanding AI landscape, auditors benefit from distinguishing between several types of AI agents, each with different capabilities and control implications. Singular task agents differ from Agentic AI, as Agentic AI includes autonomous capabilities being performed by multiple proactive agents interacting with each other with minimal human input. AI agents are goal-oriented and can be created individually to perform specific tasks on behalf of the user. Generally, AI agents can be divided into the following categories (from simple to more advanced):

- **Retrieval agents:** Retrieve information from grounding data, reason, summarise, and answer user questions.
- **Task agents:** Take actions when asked, automate workflows and replace repetitive tasks for users.
- **Autonomous agents:** Operate independently, dynamically plan, orchestrate other agents, learn and escalate.

The different agent distinctions help IA determine the level of supervision required, the potential risks introduced, and the advisory and assurance procedures necessary.

Figure 1: **Concept of AI**



Artificial Intelligence

Technology that enables machines to imitate human intelligence and automate complex tasks, such as decision-making and pattern recognition (e.g. predictive maintenance, customer behavior prediction).



Machine Learning

An AI technique in which systems learn from data to improve predictions without explicit programming (e.g. anomaly detection, maintenance planning, demand forecasting).



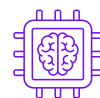
Deep Learning

Advanced machine learning using neural networks for large datasets and complex tasks such as speech recognition and image processing (e.g. chatbots, quality control, self driving cars).



Generative Artificial Intelligence (GenAI)

AI that creates new content, such as text, images, or data, by learning patterns from existing datasets (e.g. synthetic video creation, product design, content writing). The use of prompts, a clear instruction or question that guides a GenAI's response, is a well-known method of GenAI applied in practice.



Agentic Artificial Intelligence (Agentic AI)

systems that can autonomously execute tasks, orchestrate workflows, retrieve data, and interact with enterprise systems with varying degrees of autonomy.

Where human judgement remains essential

The adoption of AI in IA does not diminish the need for auditor expertise. Human judgement remains indispensable in areas such as:

- interpreting anomalies in context rather than treating them as findings;
- challenging model assumptions, data provenance, and the relevance of outcomes;

- ensuring proportionality and fairness when AI highlights outliers or behavioural patterns;
- applying ethical considerations when sensitive risks or people-related data is involved;
- avoiding that hallucinations appear in the AI output.

AI reshapes how auditors work, but it does not replace auditors' exercising professional judgement.

The dual role of AI in Internal Audit

AI influences IA in two primary ways: it supports the audit function in carrying out its own work, and it becomes an audit object, part of the audit execution of business processes. Both dimensions are increasingly relevant as organisations integrate digital systems, automated controls, and decision-support models into their operations.

1. AI supporting Internal Audit operations

AI enhances the efficiency, coverage, and consistency of IA activities across the entire audit lifecycle. In practice, this aligns with how AI is applied across key IA process steps.

- **Strengthening risk assessment and planning:** AI supports risk based planning by analysing large volumes of internal data (e.g. transactions, prior audit results, control metrics) and external inputs (e.g. regulatory developments, industry trends). Predictive analytics and machine learning techniques help identify patterns and emerging risk areas, enabling IA to prioritise and refresh audit plans beyond static annual cycles.
- **Enhancing audit testing and fieldwork:** During audit testing, AI enables more comprehensive analysis by applying techniques such as anomaly detection, clustering, and pattern recognition to full data populations rather than limited samples. For example, AI can analyse all transactions or user activities to highlight exceptions or unusual behaviour that warrant further investigation.
- **Improving compliance and control testing:** In compliance and control testing, AI can review large volumes of policies, procedures, and regulatory documentation using Natural Language Processing (NLP), supporting ongoing compliance monitoring and detection of regulatory changes or deviations from required controls.
- **Supporting reporting, documentation, and quality assurance:** AI supports reporting by structuring analysis results into draft findings, summaries, or visualisations, improving consistency and efficiency. In addition, AI can support quality assurance by scanning engagement files to identify missing documentation, inconsistent conclusions, or deviations from methodology, contributing to the continuous improvement of IA processes.

Across all these use cases, AI supports auditors by enhancing efficiency. Auditors remain fully accountable for interpretation, validation, professional judgement, and decision making. A more detailed explanation of how AI supports each phase within IA is provided in [Chapter 3](#).

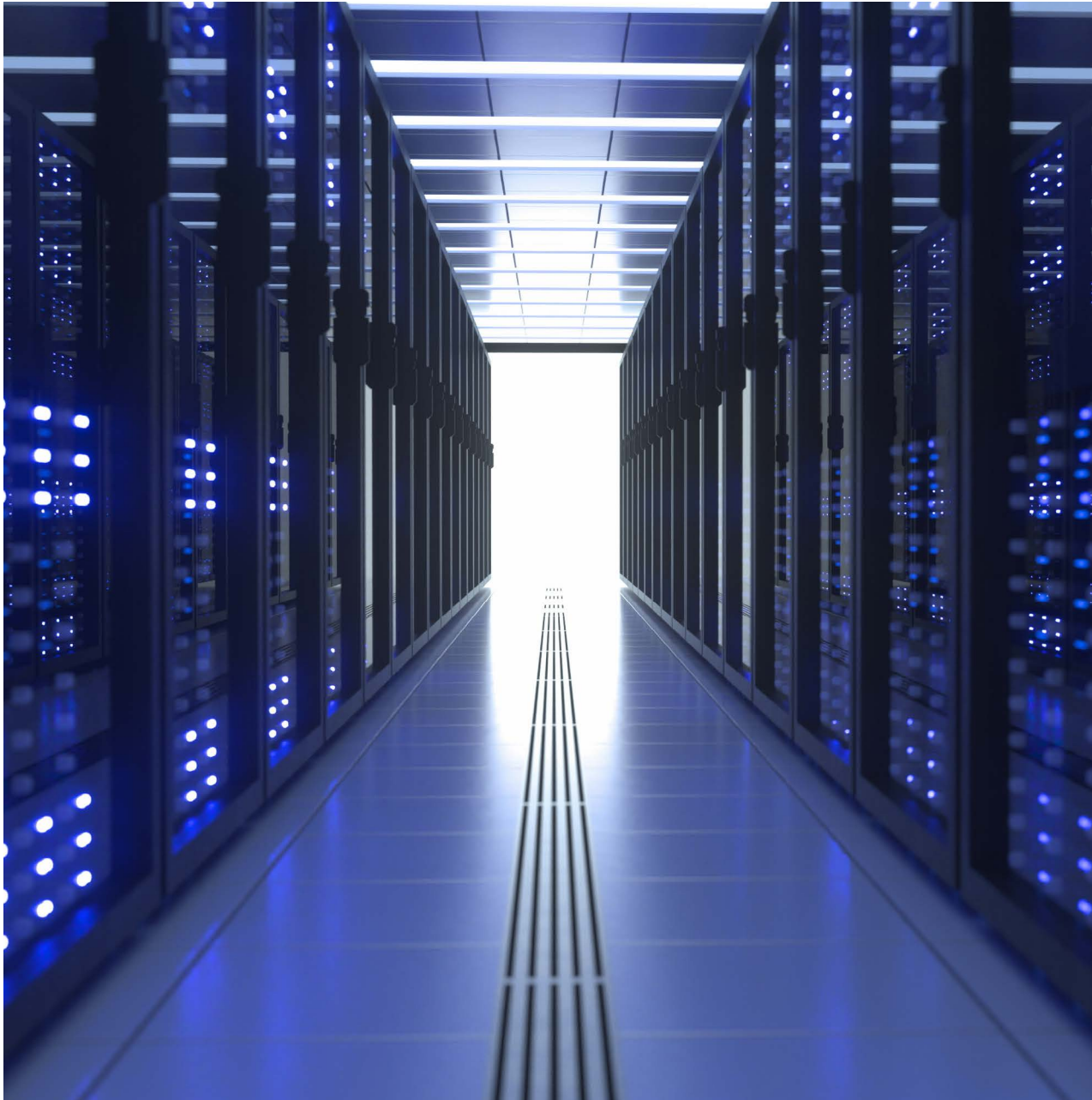
2. AI as an object of audit

As AI systems are increasingly adopted across first and second line functions, IA must assess whether these systems are reliable, ethical, and appropriately governed. This expands Internal Audit's scope to include a review of model risk management practices, such as the quality of underlying data, how models are trained, how performance is monitored over time, and whether changes affecting model behaviour are timely identified and addressed.

IA must also evaluate transparency and explainability, particularly where AI influences customer outcomes, employee related decisions, or risk mitigation activities. In addition, auditors need to test the effectiveness of controls over access, security, and override mechanisms, with particular attention to agentic or semi autonomous systems.

A further area of focus is identifying governance and accountability gaps, including clarity over ownership and responsibility for AI agents and other GenAI applications embedded in business processes. IA should also review compliance with relevant regulations, such as emerging EU requirements for high risk AI systems, with attention to documentation, human oversight, and alignment between intended and actual use.

IA therefore plays a pivotal role in supporting responsible AI adoption by ensuring appropriate governance, accountability, and safeguards are in place. More detailed information into AI governance is provided in [Chapter 4](#).



Applying the same standard internally: auditing AI while using it

Auditing AI requires IA to look beyond traditional process and control assessments and into how AI systems are implemented and used to support decisions. This includes understanding what decisions AI influences, what data it relies on and how outcomes are generated. When AI is used by the business, it is essential to keep a critical eye on topics such as data quality, explainability of outcomes, ethical safeguards, and the effectiveness of human controls around AI-driven decisions. These insights provide a practical reference point for how AI should be governed and applied responsibly across the organisation.

That same discipline must also apply when IA uses AI within its own activities. If the function expects the business to demonstrate control, transparency, and accountability over AI systems, it must hold itself to the same standard. This means ensuring that AI use within IA is deliberate, well-documented, and subject to review, rather than informal or ad hoc.

In practice, this requires IA to clearly define where AI is used in the audit process and for what purpose, such as supporting risk identification, summarising audit evidence, or drafting initial observations. For example, when generative AI is used to summarise policy documents or propose draft findings, auditors should document the prompts applied, review outputs against source documentation, and record their professional judgement. Similarly, when predictive AI models support audit prioritisation, auditors should understand and be able to explain the data inputs, assumptions, and limitations involved. By continuously reviewing the AI practices and critically challenging both inputs and outputs, IA demonstrates that accountability remains firmly with the auditor.

03 How AI supports each phase of the Internal Audit lifecycle

AI in audit planning

How AI supports audit planning

AI can enhance risk-based planning by analysing large volumes of internal and external data to identify patterns, trends, and emerging risks that may not be visible through traditional approaches. Rather than replacing traditional risk assessment approaches, AI acts as a challenger to existing assumptions by highlighting patterns or emerging risks that may warrant reconsideration of previously agreed audit priorities.

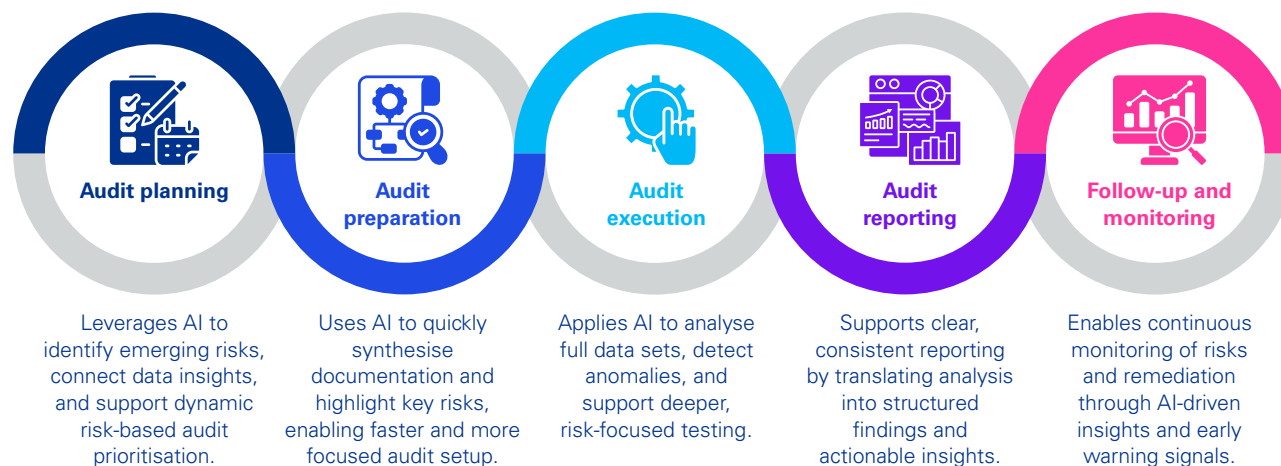
Used responsibly, AI can:

- surface weak or emerging risk signals earlier;
- connect disparate data points across the organisation;
- challenge static, assumption-driven audit plans.

Beyond risk assessments, AI can streamline internal audit planning and coordination. For example, AI tools can support scheduling meetings and stakeholder alignment by analysing calendar availabilities and proposing optimal time slots, while also assisting in drafting and tracking communications with auditees. Furthermore, AI can support the preparation of documentation requests by generating structured document requests based on audit scope, prior engagements, and risk areas. In addition, AI can assist in drafting key planning documents such as the engagement letter by suggesting standardised sections, aligning content with prior audits, and embedding relevant risk considerations.

Typical applications

- **Identifying recurring risk themes:** AI can review historical audit results, incidents, and management reports to produce clear thematic summaries and trend overviews. For a client, this meant using AI to scan several years of audit reports and issue logs, resulting in a consolidated view of recurring control weaknesses that had previously only been visible at individual audit level.
- **Supporting risk assessment:** By continuously reviewing key risk indicators and internal signals, AI can help generate regularly updated risk profiles and highlight emerging trends. In practice, this allowed a client's audit team to receive periodic risk snapshots, which supported timely adjustments to audit focus as business conditions changed during the year.
- **Risk-based prioritisation of the audit universe:** AI can support audit planning by combining current risk signals, control issues, and business changes into a refreshed prioritisation output, rather than relying on static annual plans. For a client, this resulted in a more current audit plan that shifted attention toward higher-risk areas while reducing effort spent on activities with limited risk exposure.



Role of the auditor

AI provides inputs to audit planning but does not make planning decisions. Auditors remain responsible for:

- assessing whether AI identified risk signals are relevant, credible, and aligned with the organisation's strategy and risk appetite;
- challenging AI outputs where data limitations, assumptions, or potential biases could distort prioritisation;
- combining AI insights with professional judgement, stakeholder input, and business knowledge when shaping the audit plan.

Audit planning decisions must remain well reasoned, transparent, and clearly documented, and must not be driven by AI outputs in isolation.

Practical impact for Internal Audit

In practice, the use of AI changes how audit planning is performed, not who remains accountable for it. Instead of relying primarily on periodic risk assessments and historical information, IA gains a more current and evidence driven view of risk developments across the organisation. This allows audit teams to spend less time collecting and reconciling information and more time discussing what the observed signals actually mean for the audit plan.

AI supports more timely adjustments to audit priorities, for example by highlighting rising risk indicators, recurring issues, or shifts in control performance during the year. As a result, audit plans become more responsive and better aligned with how risks evolve in reality, rather than being fixed once a year. This also enables more informed discussions with management and audit committees about why certain areas are included, deferred, or reprioritised.

At the same time, auditors must remain alert to limitations in the data and models used. Data quality, coverage gaps, and implicit assumptions can influence outputs and must

be explicitly considered when interpreting results. Final audit planning decisions therefore continue to combine AI insights with human judgement, professional scepticism, stakeholder input, and organisational context. When applied in this way, AI enhances planning discipline and focus, while preserving transparency, accountability, and trust in how audit priorities are determined.

AI in preliminary audit investigation and fieldwork

How AI supports preliminary investigation and fieldwork

During the preliminary investigation phase, AI supports audit preparation by quickly synthesising large volumes of background information, such as policies, procedures, prior audit reports, issue logs, relevant regulations, and industry developments. By summarising documentation and highlighting key themes, inconsistencies, or outdated information, AI helps auditors build context early and identify potential risk areas before fieldwork starts. For example, AI can scan several years of audit reports and policies to highlight recurring control weaknesses or areas where procedures have changed but controls have not been updated.

As the audit moves into fieldwork, AI supports more data driven execution by analysing operational data such as transactions, system logs, and automated process outputs. This allows auditors to move beyond sample based testing by reviewing full data populations, identifying anomalies, trends, and exceptions, and detecting patterns that merit further investigation. For example, instead of testing a sample of transactions, AI can analyse the full population to identify unusual user activity or control breaches, enabling auditors to focus their work on the highest risk exceptions while maintaining professional judgement.

As fieldwork progresses, AI enables more comprehensive and data-driven testing, allowing auditors to move beyond traditional sample-based approaches. In practice, AI supports fieldwork by:

- analysing full data populations rather than limited samples;
- identifying anomalies, trends, and exceptions that warrant further investigation;
- recognising patterns across transactions, users, or automated processes.



"The use of AI-supported analytics during fieldwork requires careful attention to traceability, explainability, and reproducibility."

Sander Klous

In addition, AI can support audit walkthroughs by summarising process documentation and interview notes, helping auditors structure walkthrough discussions and identify potential control gaps or inconsistencies. AI can also assist in the preparation and review of audit workpapers by generating initial documentation templates and checking for completeness and consistency against audit methodology requirements. AI during fieldwork can be particularly valuable in environments where data volumes are large, processes are highly automated, or manual testing would be inefficient or incomplete. For example, supporting auditors with anomaly detection and outlier and pattern analysis.

Role of the auditor

AI supports auditors but they remain responsible for:

- interpreting results and assessing their relevance;
- determining root causes of identified issues;
- validating exceptions and designing appropriate follow-up procedures.

As AI-supported analyses become more embedded in fieldwork, careful attention is required to ensure the reliability of audit evidence.

Auditors must be able to demonstrate which data sources were used, how analyses were performed, and how specific results were generated.

Practical impact for Internal Audit

In practice, AI allows auditors to enter and progress through fieldwork better prepared and more focused. Less time is spent on orientation and routine testing, enabling greater emphasis on substantive risk areas and insight generation. By extracting key themes across documentation and data, identifying potential gaps in controls or evidence, and reducing manual review effort, AI supports IA in delivering deeper insights while maintaining audit quality and professional judgement.

AI in audit reporting

How AI supports audit reporting

AI can support the reporting phase by helping auditors translate detailed fieldwork results into clear, structured, and consistent audit messages. Outputs from testing and analysis can be organised into draft findings, structured observations, or management summaries, supporting a consistent tone and format across reports.

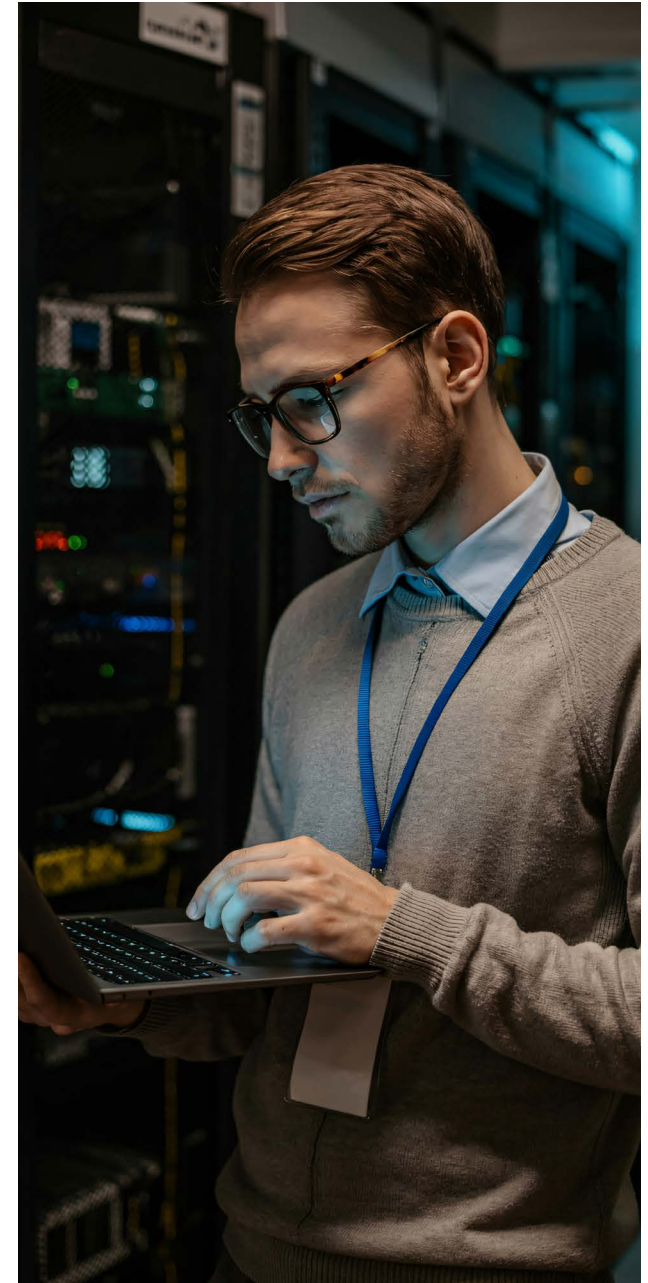
Typical applications include drafting first versions of audit findings or executive summaries, converting data heavy analyses into accessible plain language explanations, and supporting the preparation of visualisations that highlight trends and key observations for decision making. By handling these preparatory activities, AI helps audit teams move more efficiently from analysis to communication, while auditors remain responsible for final conclusions, wording, and message impact.

Role of the auditor

Final audit reports must always be:

- balanced, factual, and evidence-based;
- clearly attributable to professional judgement;
- reviewed and approved by auditors.

Auditors must critically assess AI-generated outputs to ensure accuracy, completeness, and appropriate nuance. This includes confirming that findings are supported by sufficient evidence, that conclusions are proportionate to the issues identified, and that wording reflects the organisational and stakeholder context in which the report will be read. For example, auditors must validate whether these outputs are accurate, evidence-based, and compliant with quality standards before including it to the final audit report. AI can further support the quality assurance (QA) review process by assessing draft reports against internal standards, identifying inconsistencies in terminology, structure, or rating logic, and highlighting



areas where supporting evidence may be insufficient or unclear. This helps QA reviewers focus their efforts on higher risk areas while maintaining overall report quality and compliance.

Practical impact for Internal Audit

In practice, the use of AI helps make reporting faster and more consistent, reducing time spent on drafting and reworking text. This reduces time spent on drafting and formatting which allows auditors to focus more on the clarity, impact, and relevance of audit messages, as well as on effective engagement with management and senior stakeholders.

AI in audit evaluation & follow-up

How AI supports continuous monitoring, evaluation and follow up

In a continuous auditing and monitoring context, AI supports IA by enabling ongoing visibility into risk developments and control performance, rather than relying on periodic, point in time assessments. By continuously analysing operational data, remediation information, and key risk and control indicators, AI helps IA identify changes in risk exposure as they occur and assess whether controls and mitigation actions remain effective over time.

AI can support evaluation activities by monitoring trends across audits, issues, and risk indicators, highlighting shifts that may indicate emerging risks or weakening controls. It can identify recurring issues, compare outcomes across entities or processes, and flag deviations from expected patterns that merit further attention. This provides IA with a more dynamic and forward looking view of the risk landscape.

Within follow-up activities, AI enables a more proactive and risk-focused approach to monitoring remediation. Instead of relying on manual status updates, AI can continuously track signals linked to agreed actions and control improvements, for example by:

- monitoring data and key control indicators associated with remediation actions;
- identifying early warning signals when risks re-emerge or controls fail to operate as intended;
- supporting exception-based follow-up for high-risk, delayed, or ineffective remediation.
- flagging overdue actions and automatically generating status update prompts or reminders for responsible stakeholders, ensuring timely follow up and improved accountability.

This allows IA to shift from periodic follow-up cycles to ongoing monitoring, focusing attention where it is most needed and providing management with more timely insights. For example, AI supported monitoring allows Internal Audit to identify when certain targets are not progressing as intended.

Role of the auditor

Auditors remain responsible for deciding how AI outputs are used by:

- validating the relevance of AI-generated signals within the audit context;
- assessing whether evidence and remediation actions are sufficient;
- deciding when additional follow-up or escalation is required.

Professional judgement remains essential to ensure conclusions are evidence-based and clearly documented.

Practical impact for Internal Audit

In practice, AI strengthens Internal Audit's ability to maintain continuous oversight of risks and remediation progress without significantly increasing manual effort. Monitoring becomes more targeted, timely, and risk-driven, enabling earlier intervention and more meaningful discussions with management. This reinforces Internal Audit's role in providing ongoing insight and advisory support, while ensuring accountability and decision-making remain firmly anchored in professional judgement.

Across all phases of the IA process, planning, execution, reporting, and follow up, AI supports auditors by enhancing insight, efficiency, and focus. However, accountability for audit judgements, conclusions, and priorities always remains with IA. Consistent with professional standards, the use of AI must remain transparent, explainable, and subject to professional validation, ensuring trust in both the audit process and its outcomes.



04 Risks, limitations & governance of AI in Internal Audit

Internal Audit & AI: Risks in use and oversight

The increasing integration of AI into Internal Audit requires a dual perspective. On the one hand, auditors are expected to use AI as a tool to enhance audit efficiency, depth, and insight within IA practices. On the other hand, IA has a critical and independent role in auditing the organisation's use of AI, ensuring that AI systems are governed responsibly, operate as intended, and comply with regulatory and ethical standards.

This chapter therefore focuses on both perspectives:

- **AI in Internal Audit:** guiding auditors in the responsible use of AI within audit activities, with focus on maintaining audit quality, professional scepticism, and control over AI-assisted outputs.
- **Auditing AI systems:** providing a framework for assessing risks, governance, and controls related to AI deployed across the organisation, ensuring these systems are transparent, reliable, compliant, and aligned with organisational values.

By combining these perspectives, IA can both leverage AI effectively and provide clear assurance and advice over its use.

Regulatory & compliance exposure

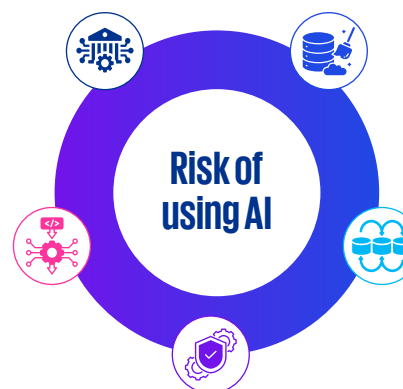
Evolving requirements (e.g. GDPR, AI Act, and sector regulations) place new demands on transparency, documentation, and data handling. IA must assess whether AI use cases, vendors, and governance structures meet compliance expectations. Moreover, AI systems introduce new security and privacy vulnerabilities, including model-level attacks and unintended exposure of sensitive data, which IA must consider when evaluating compliance and control environments.

Data quality dependencies & Garbage In, Garbage Out (GIGO)

AI-driven analyses rely heavily on complete, accurate, and current data. In line with the Garbage In, Garbage Out (GIGO) principle, poor data quality can distort outcomes, weaken risk assessments, and create assurance blind spots across multiple interconnected systems. Consequently, as with any audit, the internal auditor should apply professional scepticism, especially when the data is analysed by AI.

Over-reliance on AI outputs

Auditors may unintentionally reduce professional scepticism when AI tools appear efficient or objective. Unvalidated outputs, especially from generative models, can lead to flawed conclusions, inaccuracies in reports, or gaps in assurance. Therefore, it is important to keep a human-in-the-loop when AI outputs are used, to ensure that the generated content is correct.



Vendor & model dependency

Increasing reliance on external AI platforms reduces the organisation's control over models, data flows, updates, and availability. This complicates continuity planning and introduces concentration risks relevant to assurance. Additionally, AI-generated outputs may raise intellectual property and ownership questions, particularly when models are provided by third parties.

Bias & explainability

AI models may reinforce existing patterns in data while offering limited insight into how decisions are made. This reduces transparency, impairs auditability, and challenges the ability to assess fairness, reliability, and control effectiveness. To maintain explainability and increase insights, it is recommended to request AI to provide transparency on how outputs are derived, including referenced sources used that generate the output. The authenticity and relevance of these sources must always be critically assessed by human reviewers. In addition, creating strong quality review agents within agentic AI workflows can decrease the likelihood of bias and support consistent oversight.

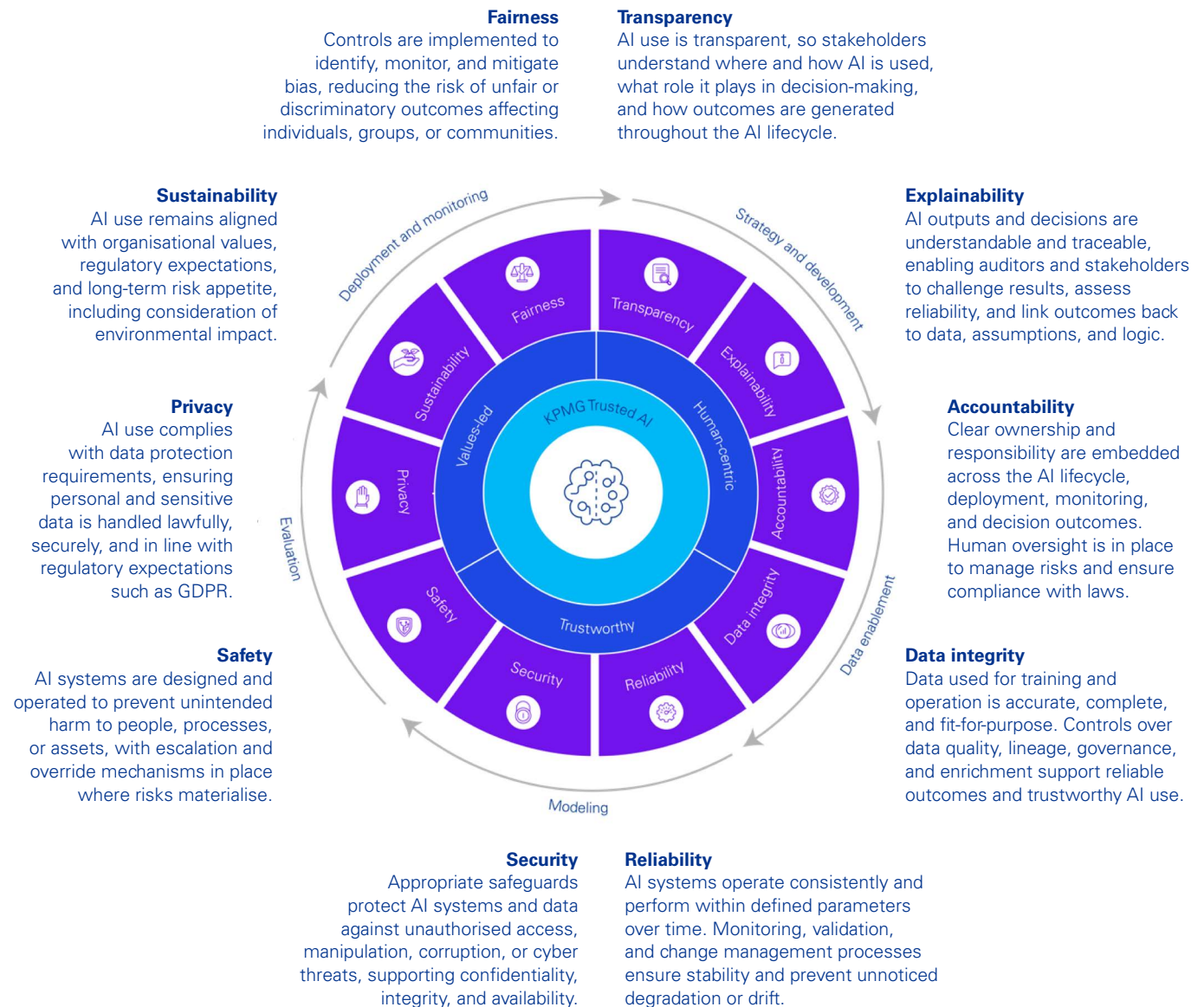
Trusted AI principles wheel

Trusted AI framework: the role of Internal Audit

The Trusted AI framework sets out key principles that guide the responsible design, deployment, and use of AI across the organisation. From an IA perspective, Trusted AI is not assessed as a theoretical concept, but through concrete audit activities. The assessment spans the full AI lifecycle, including strategy and development, data enablement, modelling, deployment, and ongoing monitoring. IA reviews whether AI solutions are developed and operated as aligned with the Trusted AI framework.

In practice, IA assesses these principles by embedding them into regular audit work. This includes testing governance frameworks for AI, reviewing policies and standards, evaluating model documentation and change management processes, assessing data quality and lineage, and verifying that monitoring and escalation mechanisms are in place. IA also reviews the oversight of third-party AI providers and evaluates whether controls remain effective after AI solutions are deployed, not just at the point of implementation.

Where appropriate, IA can support the organisation through targeted AI governance workshops or advisory engagements. These activities help management and stakeholders understand Trusted AI expectations, clarify roles and responsibilities, and identify gaps in governance or control design before risks materialise. By consistently applying Trusted AI principles through concrete assurance activities, IA helps ensure that AI systems are not only effective and innovative, but also well controlled, compliant, and trustworthy. This enables Internal Audit to provide management and governing bodies with clear, practical assurance that AI is being used responsibly and in line with the organisation's values, risk appetite, and regulatory obligations, in line with the accountability principle of the Trusted AI framework.



Governing AI responsibly

As AI increasingly supports or automates audit decisions on both process and control levels, responsible governance becomes a priority for IA. Effective oversight means more than confirming that policies exist. It requires assessing whether governance structures, controls, and assurance practices are embedded in how AI systems are designed, used, and monitored. Strong AI governance gives IA a clear and auditable framework to evaluate decision quality, compliance, and trust.

Well-designed governance links model oversight, ethical principles, and human judgement to existing organisational and professional standards. This enables IA to assess whether AI decisions are transparent, responsibilities are clearly assigned, and escalation and override mechanisms work in practice. As a result, audits can be more focused and discussions with management more valuable.

Model governance

Model governance provides IA with a structured way to assess AI systems across their lifecycle, from development and validation to use and retirement. It translates technical complexity into clear audit criteria and supports consistent assurance over AI use. By grounding audits in these elements, IA can provide concrete assurance that AI systems are controlled, explainable, and aligned with organisational expectations.

Key aspects of model governance that are particularly relevant for IA include the following:

Clarity of design and intent

Well maintained documentation describing the model's objective, scope of use, underlying logic, and known limitations allows auditors to assess whether the model is used as intended and whether reliance on its outputs is appropriate.

Clear ownership and responsibility

Defined roles, decision rights, and escalation mechanisms make it possible to determine who is accountable for model behaviour, outcomes, and corrective actions when issues arise.

Stability and performance over time

Evidence of validation, scenario testing, performance tracking, and controlled updates supports assurance that the model continues to function as expected and does not degrade unnoticed or drift from its original purpose.

Sound management of data inputs

Controls over data sourcing, quality checks, and access rights enable auditors to determine whether model outputs are based on accurate, relevant, and authorised data.

IA should also evaluate whether these governance principles are translated into effective operational controls. This includes assessing if documentation is kept up to date, whether key parameters and changes are properly logged, and monitoring practices that exist to identify unexpected behaviour or declining performance. In addition, auditors should review if contingency and safety measures are defined and tested, clarifying how decisions are handled if a model becomes unavailable or produces unreliable results. Equally important is confirming that responsibilities across model owners, developers, and oversight functions are understood and applied throughout the model's lifecycle.

Taken together, these practices enable IA to assess the use of AI with greater precision and confidence, ensuring that AI supported decisions remain traceable, understandable, and consistently governed within the organisation's overall control framework.

Broader guidance on AI governance at board level is available in the following KPMG-INSEAD report: [AI Governance Principles for Boards](#), co-developed with the INSEAD Corporate Governance Centre.

Human-in-the-Loop (HITL)

Even as AI systems grow more capable, human judgement remains essential particularly for decisions that carry significant ethical, operational, or compliance implications. Organisations must define how and when humans interact with AI models, and IA should test whether these oversight mechanisms are appropriate for the associated risks. A concrete illustration of a use case emphasising transparency and human ownership is the 'AI Factory for Internal Audit'. The AI Factory is designed to be a 'junior auditor': automating repetitive tasks but always under human supervision. It can generate a large portion of audit work programmes, but every critical step requires human review and approval, especially for compliance-heavy environments, such as firms with SOX reporting requirements. If the AI Factory cannot determine a result, it signals uncertainty rather than producing an answer.

Key considerations include:

- whether humans retain decision authority for high-impact or sensitive actions, in line with the EU AI Act requirements for human oversight;
- clear thresholds for escalation when AI behaviour exceeds expected boundaries;
- availability of monitoring, override, and fail-safe controls;
- alignment of oversight levels with the risk classification of each AI system.

These mechanisms ensure AI complements professional judgement, preserving accountability, and supporting sound governance.

05 Required Capabilities

Adopting AI within IA, as well as auditing AI systems, is not merely a technological challenge. It requires a balanced development of organisational positioning, people capabilities, and audit processes. Weaknesses in any one of these pillars will limit the effectiveness and credibility of AI-enabled assurance and advice.

Positioning: mandate, access and governance

A clear mandate is the foundation for responsible AI adoption and for auditing AI used across the organisation. IA needs explicit agreement on where AI may be used, which AI systems fall within the audit scope, for what purpose, and under which conditions. This includes access to relevant data, clarity on ownership of AI tools and outputs, and alignment with broader organisational governance for AI and data. Importantly, expectations must be realistic. AI is not yet suited for highspeed, business critical decision-making without strong safeguards.

People: skills, training and mindset

The increasing use of AI both within the Internal Audit Function and across the wider organisation fundamentally changes how auditors work. As routine and repetitive tasks become lighter and more automated, and AI-driven processes become part of the audit scope, the auditor's role shifts towards interpretation, judgement, and oversight. This requires new skills, such as understanding AI limitations, validating outputs, and providing structured feedback to AI systems.

Equally important is a change in mindset. Working faster does not automatically mean working better. Audit teams need to learn how to alternate between moments of high analytical intensity and deliberate pauses for reflection and review. This rhythm supports audit quality, professional scepticism, and consistency in judgement. Leadership plays a key role here: creating acceptance for reflection as part of high-quality audit work and sustainable adoption.

Examples to implement this in the IAF are short 'pause and review' moments within the audit workflow after intensive analysis steps, and leadership reinforcing these moments as a core element of audit quality.

Process: methodology, tooling and integration

Processes must evolve to embed AI in a controlled and repeatable way, and to provide assurance over AI enabled processes embedded in the organisation. This requires methodologies that clearly distinguish between activities

where AI supports the audit work and situations where AI itself forms part of the object of audit. This starts with clearly defining which audit activities must be human led and which can tolerate higher levels of automation. Methodologies should explicitly describe the role of AI in each phase of the audit, including review points and accountability. This is consistent with the EU AI Act, which emphasises lifecycle based governance, human oversight, and documentation of how AI is designed, implemented, and monitored, reinforcing the need for IA to assess not only AI models, but also the processes and methodologies in which they are embedded. Tooling choices should support integration rather than fragmentation.

AI capabilities are most effective when embedded in existing audit workflows and documentation standards, enabling traceability, consistency, and reuse. Over time, this integrated approach allows IA to scale the use of AI without losing control or coherence.

"We are not built for continuous high intensity test work. As AI makes more tasks lighter, we need to consciously create space for reflection after intense work to create impact as an internal auditor."

Bart van Loon



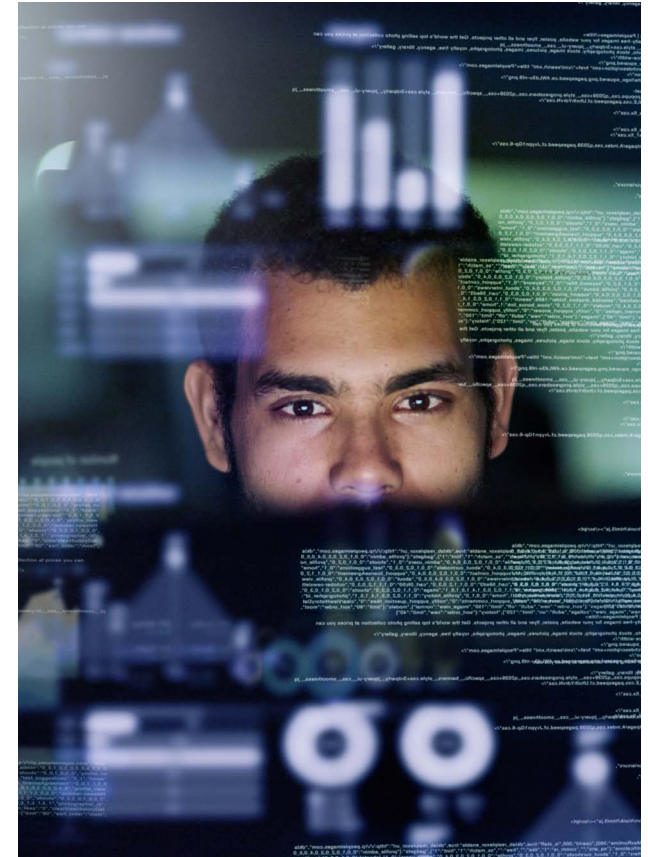
06 KPMG perspective & closing

KPMG's point of view: key takeaways & next steps

The key question for most IAFs is no longer if AI should be implemented, but how it can be applied in a way that reinforces audit quality, relevance, and credibility. AI can support IA across the entire audit lifecycle, from planning and execution to reporting and follow-up. At the same time, it is important that the fundamentals of auditing remain unchanged, as independence, accountability, and professional judgement continue to underpin effective internal auditing. AI does not replace these principles; it reshapes how they are applied in a more data-rich and fast-moving risk and control environment.

From our perspective, successful adoption is not about rushing AI implementations or adopting technology for the sake of it. Instead, it is about making deliberate, well-governed choices that support the audit mandate, include practical AI adoption and can withstand scrutiny from audit committees, regulators, and senior management. It remains crucial for IA to retain a human-in-the-loop and become a frontrunner in the organisation regarding responsible use of AI. As a result, the IAF should ensure the following:

- **AI will redefine how audits are performed, not why they are performed**
The purpose of IA remains unchanged. AI enhances methods and tools, but it does not alter the role of IA or its responsibility to provide independent and objective advice or assurance.
- **Human judgement remains central**
AI can analyse, structure, and summarise information at scale, but auditors remain responsible for interpretation, prioritisation, and conclusions.
- **Internal Audit must lead by example in responsible AI use**
As AI becomes embedded in business processes, IA has a clear role to play by using AI responsibly within the function and by providing credible advice or assurance over AI used elsewhere in the organisation.
- **The immediate focus should be on practical, controlled AI adoption**
Progress comes from starting with concrete use cases and building experience, rather than attempting large-scale transformation upfront.



How to start adopting AI within Internal Audit

Adoption works best when it starts small and purposeful. Rather than redesigning audit methodology, AI can initially support existing activities to increase efficiency in the Internal Audit process. Early application of AI allows teams to learn what works, where risks arise, and what governance is required before AI is used more widely. Early use cases create familiarity, build confidence, and provide concrete lessons about data quality, controls, and governance. Once value and reliability are demonstrated, capabilities can be scaled and embedded more structurally.

A practical starting point is to distinguish between business-critical activities and those activities where limited imperfections are acceptable. Business-critical

professional judgement, conclusions, and signoffs should remain human led with the assistance of AI where appropriate. Less critical or repetitive activities can tolerate higher levels of automation, provided there is transparency, traceability and a human-in-the-loop. This value-driven perspective helps avoid overengineering while ensuring that AI is applied where it improves audit quality or efficiency.

First action steps to consider include:

1. Select a limited number of concrete use cases

Focus on activities where AI clearly adds value today, such as document review, risk sensing, population analysis, interview creation and documentation, or drafting reports. Avoid broad experimentation without a clear audit objective.

2. Separate business-critical judgement from supporting activities

Decisions that affect audit opinions, ratings, or formal conclusions should remain human led. AI should first support preparation and analysis, not determine outcomes. Less critical and repetitive activities may allow higher levels of automation, provided that review steps are defined and implemented.

3. Define reviewer expectations upfront

Be explicit about where human review is required, what constitutes sufficient quality, and when escalation is expected. This helps prevent over-reliance on AI outputs and supports consistent application across teams.

4. Recognise the possibilities of data and model limitations

Early use often exposes data gaps, inconsistencies, assumptions, and hallucinations. Results should be analysed and used to strengthen audit planning and risk assessments, not to extend conclusions beyond what evidence supports.

5. Align AI use with audit standards and documentation requirements

AI-supported work must remain traceable and explainable. Auditors should always be able to demonstrate how results were produced and how conclusions were reached to ensure completeness and accuracy of the audit trail.

6. Scale only after value is demonstrated

Once use cases have proven reliable and useful, they can be embedded more structurally into audit processes. Expansion should follow experience and evidence, not ambition.



Key terminology

Term	Short explanation
Agentic AI	AI systems that can autonomously plan, decide, and execute tasks with minimal human input
AI Agents	Goal-oriented AI systems designed to perform specific tasks on behalf of users
Anomaly Detection	Identifying unusual patterns or outliers in data that may indicate risks
Data Governance	Framework for managing data quality, ownership, access, and usage
Data Lineage	The tracking of data origins, transformations, and movement through systems
Data Quality Dependency	The extent to which AI performance relies on accurate and complete data
Deep Learning	Advanced machine learning using neural networks for complex data processing tasks
Generative AI (GenAI)	AI that creates new content such as text, images, or code based on learned patterns
Garbage In, Garbage Out (GIGO)	Principle that poor input data leads to poor AI outputs
Hallucinations	AI generating incorrect or fabricated information that appears plausible
Human-in-the-Loop (HITL)	Human involvement in reviewing, validating, or approving AI outputs
Machine Learning (ML)	AI technique where systems learn from data to improve predictions or decisions
Natural Language Processing (NLP)	AI capability to understand, interpret, and process human language
Predictive Analytics	Using data and models to forecast future outcomes or risks
Professional Scepticism	Critical mindset used to question and validate evidence and outputs
Prompts	Instructions or inputs given to AI to guide its responses
Retrieval Agents	AI agents that search, retrieve, and summarise information
Risk-Based Planning	Prioritising audit activities based on risk levels
Trusted AI	Approach to AI ensuring it is ethical, reliable, transparent, and well-governed

Contact

IAFs that use AI by combining practical use cases with strong governance and clear human ownership will be best positioned to develop together with AI technologies. By applying AI in a controlled and responsible way, Internal Audit can strengthen its own effectiveness while setting a clear standard for responsible AI use across the organisation.

KPMG supports IAFs throughout this journey, from identifying initial use cases to embedding trusted AI responsibly within the IAF and providing assurance over AI used in the business.



Huck Chuah

Partner

Risk & Regulatory - Governance, Risk & Compliance Services

T: +31 206 564 501

E: Chuah.Huck@kpmg.nl



Pascal Raven

Senior Manager

Risk & Regulatory - Governance, Risk & Compliance Services

T: +31 206 567 546

E: Raven.Pascal@kpmg.nl



Bart van Loon

Partner

Risk & Regulatory - Governance, Risk & Compliance Services

T: +31 206 567 796

E: VanLoon.Bart@kpmg.nl



Bram Schouten

Senior Manager

Risk & Regulatory - Governance, Risk & Compliance Services

T: +31 204 262 717

E: Schouten.Bram@kpmg.nl

Acknowledgements

With thanks to Bart van Leuven, Josephine Verver and Pippi Joannes.

Generative AI was used to support the draft and final version of this whitepaper. All AI outputs have been validated and reviewed by the authors, and a human-in-the-loop approach was continuously applied.



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under licence by the independent member firms of the KPMG global organisation.