KPMG

6 key challenges of auditing AI – and how to approach them

Unlike traditional system audits, auditing AI requires new tools and ways of working. As AI adoption rises, so do the expectations on auditors to audit AI. How can we verify AI system trustworthiness, from conducting detailed reviews of the control environment, performing AI governance maturity assessments, to providing 3rd party attestation over the use of AI technology?

1 The inherent opacity of AI algorithms

Challenge faced by AI auditors

The opacity of algorithms, often termed the "black box" problem, refers to the **difficulty in understanding and interpreting the internal workings** and decision-making processes of AI systems.

This lack of explainability **complicates efforts to audit** and hold systems accountable. This can lead to **unexplainable and potentially skewed decisions**, undermining trust and accountability in AI systems.

Due to the opacity, there is also a challenge understanding **how data is being used** to make any output or AI-driven decisions and the consequences these decisions can have on data subjects.

How we can address the need for **explainability**

Conduct pre-model evaluation:

- Ensure that clear, comprehensive documentation (e.g., Model Cards) are maintained
- Ensure that the documentation is regularly reviewed and updated

Conduct post-model evaluation:

- Ensuring guardrails have been implemented
- Ensure that any output includes clear explanation and referenced
- Ensuring that there is an audit trail

Ensuring Transparency

- Assess the proactive disclosure of AI usage in generating outputs, including any human involvement
- Ensure disclosing, with clear explanations on what data and algorithm is used to make AI driven decisions

Expected benefits

- ☑ **Provides insight into how outputs are derived**
- ☑ **Promotes fair practices**
- ☑ **Improved decision-making based on understandable AI outputs**

2 Distorted AI outcomes due to biased or poor-quality data

Challenge faced by AI auditors

AI models are fundamentally reliant on the data they are trained with.

This means that **biased population data will inevitably produce unfair or discriminatory outcomes.**

Such biased outcomes can perpetuate existing inequities and contribute to discrimination.

How we can address the need for **fairness**

Inspect approved policy and procedures that address bias and inclusivity and identify how fairness is defined in the organisation's context.

Assess ground data for bias:

- Verify grounding data covers all customer profiling factors
- Investigate whether data have been left out intentionally

Document evidence of counterfactual fairness

- Fairness metrics analysis (using tools & techniques)
- Run controlled test scenarios with synthetic profiles to check for disparities

Verify if there is a model card outlining the data sources, risks, and known biases.

Expected benefits

- ☑ **Mitigates the risk of biased outcomes**
- ☑ **Enhances transparency and trust among stakeholders and users of AI**
- ☑ **Prioritising fairness creates long-term business value**

3 The challenge of assigning ownership in AI models

Challenge faced by AI auditors

Traditional audit models face **challenges in assigning ownership** when AI systems operate autonomously or incorporate third-party models, causing **unclear responsibility among developers, data providers, and system deployers.**

Unclear ownership of AI related risk. Traditionally, cybersecurity risk is owned by CISO or IT departments. However, AI risk extends beyond traditional cybersecurity.

How we can address the need for **clear accountability** among stakeholders

Ensure there is proper oversight with respect to AI management. (e.g. The organisation's Terms of Reference (TOR) for both the Board, or a committee delegated by the Board, and Senior Management)

Ensures that the risks related to AI systems are periodically reviewed with senior management and the Board.

Ensure AI system/ process/ risk owner is assigned at line 1 functions.

Design for Human in the Loop (HITL) across the lifecycle.

Mandate manual validation for high-stakes decisions (e.g. large investment decisions).

Ensure that Line 1 owns AI related risks since the use of AI solutions are **embedded into core business processes.**

Expected benefits

- **Responsible deployment of AI systems**
- **Holds stakeholders accountable for the effects of AI**
- **Trust building among internal and external stakeholders**

4 Restricted visibility into the underlying models and data

Challenge faced by AI auditors

Many clients may be **reluctant to share access to their proprietary models and data with AI auditors due to concerns over confidentiality and intellectual property protection.** This restricted visibility also applies when **using third-party models**, further complicating the auditors' ability to ensure system integrity and functionality without direct access to the underlying components.

API access for query responses offers a viable solution for AI auditors. However, it is crucial that these APIs are designed and integrated into the system from the outset.

Expected benefits

- **Greater transparency into model algorithm**
- **Access for auditors into proprietary or third-party AI models**

How we can address the need to **embed auditability** into API design from the outset

Ensure organisations design and implement the following:

- Build auditability into the design of the model by allowing for audit hooks and API access.
- Implement a query-based system to allow auditors to interact with models indirectly, ensuring thorough evaluations without compromising proprietary information.
- Provide comprehensive documentation for APIs, including usage instructions, endpoints, and data formats, to facilitate understanding and traceability.
- Utilise model cards to document and evaluate third-party generative AI models, providing transparency about their intent, data, architecture, and performance.
- Use automated tools for evaluating LLMs.
- During audits, there may be a need to query third-party models (e.g. compare expected output with actual output). Hence, there is a need to plan for token costs (input and output) to optimise the query responses that the auditor needs.

5 The subjective nature of ethics

Challenge faced by AI auditors

Due to **the subjective and complex nature of applying moral principles,** it is difficult to determine whether AI systems truly align with ethical expectations.

The lack of universal ethical standards and the **difficulty of translating abstract moral principles into measurable indicators** makes it challenging to translate values into clear auditable criteria.

How we can address the need for **ethical AI** audit objectives

- Ethical considerations should be addressed before deploying an AI system and continuously maintained.
- Involving a multidisciplinary team to ensure diverse perspectives are being considered.
- Breaking down broad ethical goals into specific, measurable criteria that can be verified within the organisation's context, ensuring that these objectives effectively guide responsible AI development.
- Use industry recognised standards such as ISO 42005 AI system impact assessment to analyse potential harms and benefits for AI systems.

Expected benefits

- ☑ **Ensuring they are acceptable and beneficial to society**
- ☑ **Increases accountability in data and algorithms**
- ☑ **Translating goals into actionable and auditable criteria**

6 The non-deterministic and dynamic nature of AI systems

Challenge faced by AI auditors

AI systems continuously learn from new data, experiences, and interactions, which means **they may not always produce the same output given the same input.**

This variability may undermine the predictability and stability of the system's performance, potentially posing **challenges for maintaining quality control and ensuring reliable outcomes over time.**

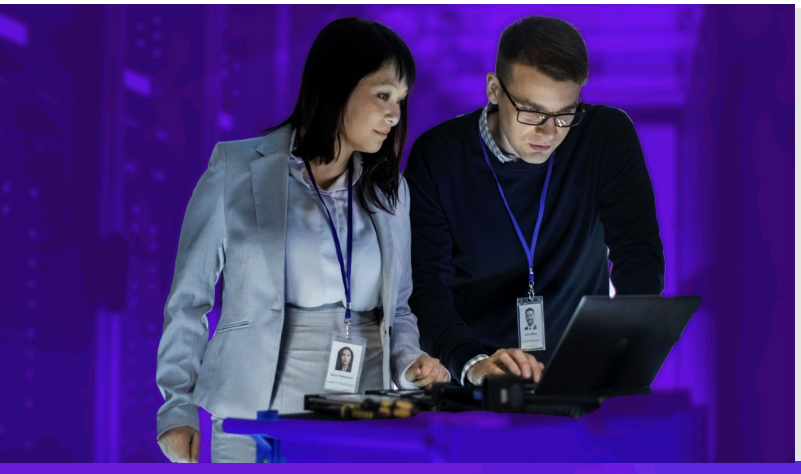
How we can address the need for **continuous monitoring and regular audits**

- Verify that the organisation is performing continuous monitoring/ regular audits and promptly addressing any identified issues
    - Output stability
    - Drift detection
    - Security anomalies
    - Boundary of variability
    - Compliance requirement
    - Threshold adjustment
- Auditors should be continually trained updated on AI advancements and best practices.

Expected benefits

- ☑ **Ensures consistent system performance**
- ☑ **Enables early detection & correction**
- ☑ **Enhances auditors' proficiency**

What's next: How the auditor's role will evolve



Higher maturity of AI adoption demands higher complexity and rigor of controls. As AI becomes increasingly embedded in organisations, the role of auditors will expand in scope and sophistication – and constant upskilling is key to keeping pace in this dynamic landscape.

Today

- Rising demand for AI audits
- Growing emphasis on ethics
- Increasing regulations and frameworks

In 1 years

- Increased automation tools and technologies
- Deeper understanding of AI algorithms and technologies will be required
- Emergence of new regulations and guidelines to govern AI audits

In 3 years

- Specialised certifications or qualifications for auditing AI will emerge
- Enhanced collaboration with data scientists
- Stronger emphasis on ethical considerations

In 5 years

- AI-driven auditing
- Consider areas that are impacted by future AI strategy and ensure it is covered as part of risk management and governance
- Likely see the rise of global standardisation and a unified approach to AI auditing

KPMG

Be in Front

You can make risk less risky with AI.

At KPMG in Singapore, we help organisations navigate AI complexity with confidence – through trusted AI methodologies, tailored governance models, and deep expertise in emerging technologies. Whether you're building AI literacy, refining your governance frameworks, or embedding intelligent assurance into your processes, we're here to help.

Book a consultation

Ready to go beyond compliance and tackle AI risks strategically with confidence? Schedule a one-on-one conversation with us today.

Gerry Chng
Partner
Head of Cyber, Advisory
KPMG in Singapore
E: gerrychng@kpmg.com.sg

kpmg.com/sg/ai-in-internal-audit