The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 5/2026
11 May 2026

FROM ALGORITHMS TO ACCOUNTABILITY:
Internal Audit's Role in Governing AI

The Institute of Internal Auditors Malaysia

Technical Newsletter

Issue 5/2026
11 May 2026

Artificial intelligence (AI) is increasingly embedded within organisational decision-making. From fraud detection and credit risk assessments to predictive maintenance and cybersecurity monitoring, AI systems now influence how organisations allocate resources, evaluate risks and interact with customers. While these technologies bring powerful capabilities, they also introduce governance challenges that traditional control frameworks were not designed to address. Issues such as algorithmic bias, decision-making that is difficult to explain and reliance on large volumes of data can create risks that are difficult to detect through conventional audit approaches.

As AI adoption accelerates, organisations must ensure these systems operate in a manner that is transparent, reliable and aligned with ethical and regulatory expectations. In this evolving environment, Internal Audit (IA) has an important role to play. By providing independent assurance over AI governance structures, model oversight processes, and data management practices, internal auditors can help organisations move from AI adoption to accountable deployment.

1.0 A NEW RISK LANDSCAPE

AI introduces a category of risk that differs from traditional information systems. Conventional IT systems operate based on predefined rules and predictable outputs. In contrast, machine learning models are derived from patterns in data and their performance may change over time as data, environments or assumptions shift. This dynamic behaviour creates new forms of uncertainty.

One widely discussed concern is algorithmic bias. When models are trained on historical datasets that reflect past decisions or social patterns, they may inadvertently reproduce those patterns in future outcomes. In areas such as lending, hiring, or insurance, this can create significant legal and reputational consequences.

Another challenge relates to model transparency. Many AI systems, particularly those based on advanced machine learning techniques do not easily reveal how a specific decision was generated. This lack of explainability can complicate regulatory compliance and make it difficult for organisations to justify outcomes to regulators or affected stakeholders.

AI systems are also highly dependent on data quality and governance. If training datasets contain inaccuracies, incomplete information, or hidden biases, the reliability of the model's outputs may be compromised. Over time, models may also experience model drift, where performance gradually deteriorates as business conditions or data patterns change.

These risks highlight the importance of establishing governance structures specifically designed for AI. Without clear oversight mechanisms, organisations may unknowingly rely on automated decisions that they do not fully understand.

> **" As algorithms increasingly influence organisational decisions, IA has a key role in ensuring that technological capability is matched by governance accountability "**

2.0 WHY TRADITIONAL AUDIT APPROACHES ARE NOT ENOUGH

IA function has long provided assurance over IT controls, cybersecurity practices and data governance. However, evaluating AI systems requires expanding beyond traditional audit methodologies.

Conventional IT audits typically focus on system access controls, configuration management, and change management processes. While these remain important, they do not fully address the governance issues associated with algorithm-driven decision-making. For instance, auditing an AI-enabled process may require understanding how training datasets were selected, whether models were independently validated before deployment and how performance is monitored after implementation. These considerations extend beyond traditional system controls and enter the domain of model governance and algorithm accountability.

AI initiatives also tend to be multidisciplinary, involving data scientists, technology teams, business units and risk management functions. Without clearly defined governance structures, accountability for AI decisions can become fragmented across the organisation. Internal auditors therefore need to broaden their assurance perspective by evaluating not only the technology but also the governance mechanisms that ensure AI is used responsibly.

" The real governance challenge of AI is not how well the algorithm performs but whether organisations remain accountable for the decisions it makes "

3.0 INTERNAL AUDIT'S ROLE IN AI ASSURANCE

IA can play a critical role in strengthening organisational oversight of AI systems. Consistent with the IIA Global Internal Audit Standards, auditors are expected to provide independent assurance over governance, risk management and internal control processes.

In my experience working with organisations adopting emerging technologies, governance discussions often focus heavily on capability and performance, while the accountability dimension receives far less attention. In the context of AI, this responsibility includes evaluating whether organisations have established appropriate governance structures for AI initiatives. Boards and senior management should define clear accountability for AI decision-making and ensure appropriate oversight mechanisms are in place.

Internal auditors should also assess model governance practices, including whether models undergo independent validation before deployment and whether organisations maintain documentation explaining model logic, assumptions and limitations.

Another important assurance area is data governance. Since AI models rely heavily on data inputs, auditors should review whether management has implemented controls over data quality, access management and data lineage (i.e. data's journey from source to final use).

Auditors can also examine whether organisations have introduced ethical safeguards governing the use of AI technologies. This includes policies addressing fairness, transparency and responsible use of automated decision systems. Such governance considerations are increasingly reflected in emerging global frameworks, including the NIST Artificial Intelligence Risk Management Framework and the OECD Principles on Artificial Intelligence, both of which emphasise transparency, accountability and trustworthy AI deployment.

By evaluating these governance mechanisms, IA can provide assurance on whether AI adoption is supported by appropriate oversight and accountability

4.0 A MOMENT OF REALISATION : WHEN AI GETS IT WRONG

(Kindly note that some details have been generalised, aggregated, or modified due to data sensitivity)

Consider an illustrative scenario involving a large retailer experimenting with an AI-driven recruitment tool. The organisation implemented an algorithm designed to screen thousands of job applications. The model analysed historical hiring data to identify characteristics associated with successful employees.

On paper, the system appeared efficient and objective. However, several months after deployment, management noticed an unexpected pattern. The algorithm consistently downgraded applications from candidates who attended certain universities. The reason was subtle but revealing where historical hiring data showed that most successful employees had graduated from a small group of institutions that the company had historically favoured. The algorithm had simply learned to replicate past decisions.

What appeared to be an objective technology had unintentionally reinforced historical hiring biases. The organisation ultimately had to withdraw the model and redesign its recruitment process. The lesson is clear: AI systems do not remove bias but they can amplify it if governance controls are weak. IA can help organisations identify such risks early by reviewing training datasets, model validation procedures and oversight mechanisms.

ANOTHER"A-HA"MOMENT : WHEN MACHINES BECOME TOO CONFIDENT

Consider another illustrative scenario involving predictive maintenance in an industrial environment. An energy company deployed an AI model to predict when critical equipment might fail. By analysing thousands of sensor readings, the system generated alerts indicating when maintenance should be performed. Initially, the model performed extremely well and helped reduce unexpected equipment downtime.

Over time however, engineers began to rely heavily on the model's recommendations. Routine inspections were gradually reduced because the algorithm was assumed to be more accurate than human judgement. Months later, a significant equipment failure occurred despite the AI system having predicted normal operating conditions. Subsequent investigation revealed that the model had been trained on historical data collected under different operating conditions. As equipment aged and operational patterns changed, the model's accuracy deteriorated but the system continued producing confident predictions.

The issue was not the algorithm alone but weak monitoring, inadequate oversight and over-reliance on the model without sufficient human accountability. This example highlights a key principle: AI models can appear highly reliable even when their underlying assumptions are no longer valid.

The Institute of Internal Auditors Malaysia

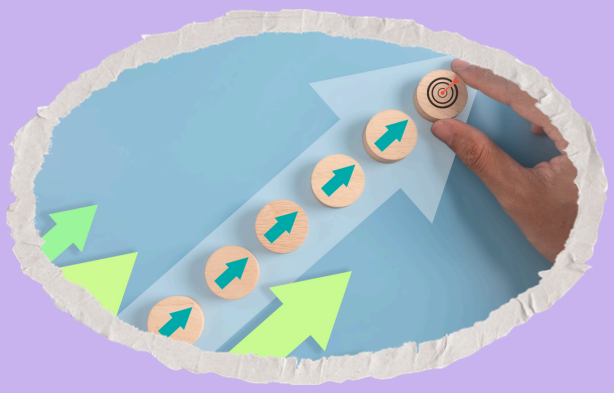
Technical Newsletter

Issue 5/2026
11 May 2026

5.0 FIVE PILLARS OF AI GOVERNANCE

> " AI may automate decisions but governance must ensure that responsibility remains human "

In order to translate governance principles into practice, organisations may consider structuring AI oversight around five foundational pillars.



i. Strategic Oversight

Boards and senior management should establish clear accountability for AI initiatives. Governance committees or technology oversight forums can help ensure AI risks are considered in strategic decision-making.

ii. Data Governance

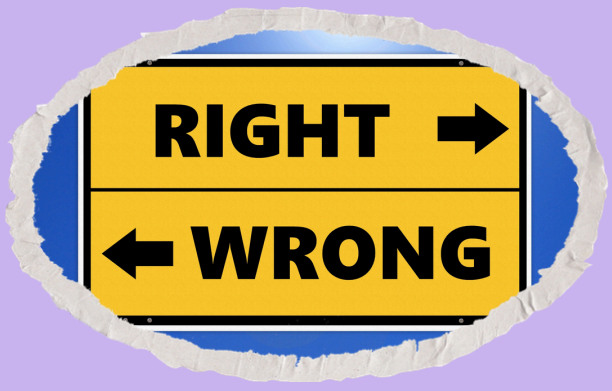
Trustworthy AI depends on high-quality data. Organisations should implement controls over data sourcing, data integrity, access management and compliance with privacy regulations.

iii. Model Transparency and Validation

AI models should undergo documented development and validation processes. Independent review of model assumptions and performance helps ensure reliability and explainability.

iv. Ethical Safeguards

Responsible AI deployment requires consideration of fairness, bias mitigation and ethical implications. Organisations should establish principles guiding acceptable use of AI technologies.



v. Continuous Monitoring

AI systems require ongoing oversight after deployment. Monitoring processes should detect model drift, unexpected outcomes and changes in operating conditions that could affect model performance.

6.0 PREPARING INTERNAL AUDITOR OF THE FUTURE

As AI becomes more prevalent across business operations, internal auditors will increasingly encounter algorithm-driven processes during audit engagements. While auditors do not need to become data scientists, they should develop a working understanding of how AI systems function, including concepts such as model training, validation and performance monitoring.

Equally important is the ability to evaluate governance structures that support responsible technology adoption. Skills in data governance, digital risk management and technology assurance will become increasingly valuable as organisations expand their use of AI.

7.0 KEY TAKE-AWAYS

i. AI presents organisations with both powerful opportunities and complex governance challenges. As AI systems become embedded in critical business processes, ensuring accountability and responsible use will be essential.

ii. IA is uniquely positioned to contribute to this effort. By providing independent assurance over governance frameworks, model oversight processes and data management practices, internal auditors can help organisations move from algorithmic innovation to accountable and trustworthy deployment.

iii. In the age of intelligent machines, effective governance is no longer only about system control. It is also about ensuring that AI is used responsibly, decisions are properly understood and can be challenged and accountability always remains with people.

Author: Javen Khoo Ai Wee, CIA, CISA, AAIA, CFE, ISC2 CC
CMIIA Membership No. 211787

REFERENCES

[1] National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.

[2] Organisation for Economic Co-operation and Development (OECD), OECD AI Principles, adopted 2019 and updated 2024.

[3] The Institute of Internal Auditors (IIA), Global Internal Audit Standards, 2024 edition, effective 9 January 2025.