

Technical Newsletter

Issue 10/2026
(October/2026)



From AI Users to AI Assurance Providers

The Next Step for Internal Auditors

Technical Newsletter

Issue 10/2026 (October/2026)

1. Introduction

In Malaysia, artificial intelligence has moved from a concept to a key part of daily operations, especially in banking and finance. We see its impact in areas like credit decisions, fraud detection, anti-money-laundering efforts, and customer support. A survey by Bank Negara Malaysia revealed that by the end of 2024,[1] about 70% of banks and financial institutions had used at least one AI tool. As we approach the end of 2026, AI continues to gain strategic importance across Malaysia's financial sector, with more than 60% of banking institutions and insurers and takaful operators viewing AI as a strategic priority over the next one to three years.[2]

Internal auditors already use AI for risk assessment, testing, and reporting. Now, boards and audit committees are asking them to provide independent assurance that the organisation's use of AI is properly governed and controlled. The key question is whether both internal audit functions and their organisations are ready to take on this responsibility.

This article explores how internal auditors can prepare for the likely challenges and move beyond being AI users to trusted providers of assurance over AI.

2. Why This Matters Now

First, AI regulation is becoming more stringent, and organisations face greater accountability.

Malaysia's National Guidelines on AI Governance and Ethics (AIGE), launched by MOSTI in September 2024, give seven principles for using AI safely and responsibly.[3] The guidelines are voluntary, but they show how future laws may develop. For financial institutions, Bank Negara Malaysia's August 2025 AI paper recommends risk-based controls.[4] It also says that existing rules, especially the Risk Management in Technology (RMiT) policy, should be used to manage AI risks for now.[5] Other relevant laws include the Personal Data Protection (Amendment) Act 2024[6], the Cyber Security Act 2024[7], and Section 213 of the Companies Act 2016 on directors' duty of care, skill and diligence[8]. Together, these rules mean that AI failures are not only operational problems. They can also create governance, compliance, and director-level risks.

Technical Newsletter

Issue 10/2026 (October/2026)

Second, organisations are using AI faster than they are putting controls in place.

In many organisations, AI has spread without a central inventory, an acceptable-use policy, or a clear owner. Assurance capability has simply not kept pace with the speed of adoption.

Third, professional standards now expect more from internal audit.

The Global Internal Audit Standards (GIAS 2024)[9] require internal audit to address significant emerging risks, to maintain the competencies its plan demands, and to give the board a clear-eyed view of how those risks are managed. AI is exactly the type of risk covered by the Standards. Internal audit already has a duty to provide assurance over it.

3. From AI User to AI Assurance Provider

It is useful to separate the **two roles** the profession is being asked to play.

Internal audit as a user of AI. This is where most internal audit teams start, and it brings real benefits. Teams use data tools and AI to check every transaction instead of just a sample, spot unusual items that need a closer look, speed up risk assessment and audit planning, and help write working papers and reports. When auditors use AI tools in their own work, they also learn how AI works, and that knowledge prepares them for the second role. But knowing how to use AI is not the same as being able to audit it. The two are different, and they should not be mixed up.

But using AI tools also brings risks that auditors do not always see. When an auditor pastes client data, payroll files, or customer records into a public AI tool, that data may be stored on outside servers, used to train the tool, or kept longer than expected. In Malaysia, this can create problems under the PDPA 2010, as amended in 2024, and it can also breach the client's own confidentiality rules or the terms of the audit engagement. Other common gaps include using personal accounts instead of approved company tools, not knowing whether the tool's provider keeps the data, and relying on AI-drafted findings without checking them.

Technical Newsletter

Issue 10/2026 (October/2026)

Internal audit as an assurance provider over AI. How can internal auditors provide credible assurance if they lack sufficient AI expertise? Equally, how can they communicate that assurance effectively to the board when their own AI knowledge may also be limited? Assurance on AI only works if both the board and the auditors understand it well enough. Directors do not need to be technical experts, but they must know enough to ask the right questions and challenge weak answers. Auditors need deeper knowledge, because they must test the controls and stand behind their opinion. If neither side understands AI, it becomes a case of the blind leading the blind, and in the land of the blind, the one-eyed man is king. The auditor's view is accepted not because it is sound, but because no one can question it. Boards should invest in their own AI education, and audit functions should build their skills, bring in experts where needed, and be honest about what they can and cannot assure.

4. Required Capabilities

Internal auditors do not need to become data scientists or programmers. They need enough knowledge to understand AI, see where it can go wrong, and test whether it is being controlled. The main areas are:

1. The basics of how AI works. What AI is, the difference between traditional AI (which makes predictions or decisions, such as credit scoring) and generative AI (which produces text, images, or answers, such as chatbots), and how AI learns from data. The key point to grasp is that AI works on patterns and probabilities, not true understanding, which is why it can be confidently wrong.

2. The main risks. Data privacy and security, wrong or made-up answers, bias and unfair outcomes, lack of transparency (not knowing why the AI gave an answer), over-reliance by staff, dependence on outside providers, and shadow AI. Shadow AI is when staff use AI tools at work without the company's knowledge or approval.

Technical Newsletter

Issue 10/2026 (October/2026)

3. Data. AI is only as good as the data behind it. Auditors should understand data quality, where data comes from, who owns it, and how it is protected. Many AI problems are really data problems.

4. Governance and controls. What good AI governance looks like: policies, an inventory of AI tools, clear ownership, approval before use, human review of AI output, ongoing monitoring, and reporting to the board. Auditors should know what controls to expect so they can spot gaps.

5. Laws, rules, and frameworks. In Malaysia, the PDPA (Amendment) Act 2024, international frameworks such as ISO/IEC 42001 and the NIST AI Risk Management Framework[10], and the IIA's own guidance on auditing AI[11]. Auditors should also know how GIAS 2024 applies, especially on competence and the use of technology.

6. How to audit AI. How to scope an AI review, what questions to ask, what evidence to request, and how to test whether an AI system performs as intended. This includes knowing when the work goes beyond the team's skills and needs an outside expert.

7. Hands-on use. Using approved AI tools in their own work, safely. There is no better way to understand AI's strengths and weaknesses than to use it and see where it fails.

AI GOVERNANCE & RISK: THE AUDITOR'S VISUAL GUIDE



Technical Newsletter

Issue 10/2026 (October/2026)

5. Capability Development

Training is available at several levels, from free material to full certifications.

1. Professional bodies for internal auditors

- The IIA (global). The IIA, together with AI CERTs, offers an AI-Enabled Internal Audit Certificate Programme that teaches auditors to apply AI across the whole audit, from risk assessment and planning through fieldwork, reporting and follow-up. It aligns with GIAS and covers frameworks such as ISO/IEC 42001, the NIST AI Risk Management Framework, and the EU AI Act. The IIA also runs shorter online courses; for example, its "Essentials for AI Auditing" course covers AI governance, risk management and auditing techniques.
- IIA Malaysia. Worth checking its training calendar for local AI courses, webinars and conference sessions. Local courses are cheaper and cover the Malaysian context.

2. Certification for those who will lead AI audits

- ISACA's AAIA (Advanced in AI Audit). It is open to holders of an active CISA, CIA or CPA, and covers AI governance and risk, AI operations, and AI auditing tools and techniques.
- ISO/IEC 42001 courses (lead auditor or implementer), offered by certification training bodies, are useful for those who will review AI management systems.

3. Free and low-cost material

- Free reading: the IIA's AI Auditing Framework 2024 and related guidance, the NIST AI Risk Management Framework, and Malaysia's National Guidelines on AI Governance and Ethics.
- Joint webinars: the IIA and ISACA have run joint webinars on auditing AI risks, controls and ethics for internal and IT auditors.
- General AI literacy courses online, such as "Elements of AI" (free), which is a series of free online courses created by MinnaLearn and the University of Helsinki.

Technical Newsletter

Issue 10/2026 (October/2026)

4. Learning by doing

- Using approved AI tools in the team's own work, under clear rules.
- Short internal sharing sessions where team members show what worked and what went wrong.
- Working alongside outside experts on the first AI review, so skills transfer to the team.

For the board, training is usually best delivered as a short, tailored in-house briefing. Director bodies such as the Institute of Corporate Directors Malaysia (ICDM) are also worth checking for AI governance programmes aimed at directors.

Co-sourcing is one of the best ways to build AI audit skills, because the team learns by working on a real audit alongside experts, not just in a classroom. But knowledge transfer does not happen by itself. It has to be planned.

- Write it into the contract. Make knowledge transfer a stated deliverable, not an extra. Include training sessions, handover of work programmes and tools, and a debrief at the end.
- Pair people up. Assign in-house auditors to work side by side with the provider's specialists, doing real tasks rather than just observing.
- Shift the balance over time. In the first engagement, the provider leads and the team supports. In the next, the team leads and the provider reviews. Eventually the team works on its own, calling in experts only for highly technical testing.
- Document the method. Ask the provider to leave behind the audit programme, risk and control lists, testing steps and lessons learned, in a form the team can use again.
- Check progress. The chief audit executive should assess whether the team's skills have actually improved after each engagement, and adjust the plan if not.
- supports. In the next, the team leads and the provider reviews. Eventually the team works on its own, calling in experts only for highly technical testing.
- Document the method. Ask the provider to leave behind the audit programme, risk and control lists, testing steps and lessons learned, in a form the team can use again.

Technical Newsletter

Issue 10/2026 (October/2026)

Things to watch out for

- Dependence on the provider. If the provider does all the thinking, the function ends up relying on them every time. That is outsourcing, not co-sourcing.
- Choosing the right provider. Under GIAS 2024, the chief audit executive stays responsible for the work. The provider's competence, independence and objectivity should be checked, for example, whether they also sold or implemented the AI system being audited.
- Cost versus benefit. Knowledge transfer takes more time than simply letting the provider do the work, so it may cost more at first. It pays off when the team becomes self-sufficient.
- Staff turnover. If trained staff leave, the knowledge goes with them. Good documentation and spreading skills across more than one person reduce this risk.

6. Implementation Phases

Auditing AI is a journey, not a single step. Auditors should first learn the basics and understand the risks during the first phase. Next, the audit function should then control its own use of AI, assess its skills honestly, and plan training, with one person appointed to lead. It should then identify where AI is used across the organisation and help the board build a basic understanding. Next, a first advisory review of AI governance, done alongside experts through co-sourcing, gives the board early value while the team learns. Finally, with deeper training and certification, AI can then become part of the regular audit plan, and within a year or two the team can move on to assurance audits of specific AI systems, bringing in experts only for the most technical work.

As the team moves through this journey, it is important to note that AI changes quickly. The team should keep up to date through regular training and sharing, and the board should receive short updates on AI risk and how it is being managed.

Technical Newsletter

Issue 10/2026
(October/2026)

Phase	Learning Objectives	Goals
1. Learn the basics	• Complete a short AI literacy course (free online courses, IIA or IIA Malaysia webinars). • Read key guidance: the IIA's AI Auditing Framework, Malaysia's National Guidelines on AI Governance and Ethics, and the NIST AI Risk Management Framework. • Learn the main risks: data privacy and security, bias, lack of transparency, over-reliance, provider dependence, and shadow AI.	All auditors have the basic knowledge needed to talk about AI with confidence.
2. Getting house in order	• Set team rules for AI use: approved tools only, no public tools on office PCs or personal phones for audit work, mask sensitive data, share only what is needed, and check every AI output. • Where possible, use an enterprise AI tool with proper data protection terms. • Start using approved AI tools in daily audit work, such as data analysis, planning and drafting, to gain hands-on experience. • Build these rules into the audit methodology.	Internal audit uses AI safely before it audits anyone else.

Technical Newsletter

Issue 10/2026
(October/2026)

Phase	Learning Objectives	Goals
3. Assess skills and plan training	- Assess the team's AI knowledge against what is needed. - Appoint one person as the AI audit lead. - Prepare a training plan: basics for everyone, IIA AI courses for the team, and a certification such as ISACA's AAIA or ISO/IEC 42001 for the AI lead. - Decide where outside experts will be needed.	A clear realistic development plan
4. Understand AI use in the organisation	- Ask management to build, or help gather, a list of all AI tools in use, including unapproved tools, free public tools and use on phones and tablets. - Meet IT, the data protection officer, risk management and key business units to understand how AI is being used. - Support a short AI briefing for the board and senior management, focused on the questions directors should ask.	A first picture of AI use and AI risk across the organisation, shared with the audit committee.

Technical Newsletter

Issue 10/2026
(October/2026)

Phase	Learning Objectives	Goals
5. Advisory review of AI Governance	• Scope a review of AI governance covering: AI policy, inventory of tools, ownership, approved tools and enterprise contracts, data protection, controls on personal devices, staff awareness, and reporting to the board. • State clearly the criteria used: the organisation's own policies, the PDPA 2024, and published guidance. • Use co-sourcing with knowledge transfer: in-house auditors work side by side with experts, and the provider leaves behind work programmes and checklists. • Protect independence: advise, but let management own and decide the framework. Report honestly on what was covered and what was not.	First AI governance report issued to management and the audit committee.
6. Build deeper skills	• The AI lead completes a certification (such as AAIA or ISO/IEC 42001). • The team attends further IIA courses and shares lessons internally. • Add AI risks to the annual risk assessment and audit plan. • Follow up on the findings from the first review.	AI is part of the regular audit plan, and the team has an AI lead with recognised skills.

Technical Newsletter

Issue 10/2026
(October/2026)

Phase	Learning Objectives	Goals
7. Assurance audits of specific AI systems	• Audit specific AI systems that carry high risk, looking at data quality, how the system was approved, whether it works as intended, bias and fairness, human review of results, monitoring over time, and provider contracts. • The in-house team now leads, with outside experts brought in only for highly technical testing. • Continue to report honestly on the limits of the work.	Internal audit can provide both assurance and advice on AI with confidence.

7. Challenges in Implementation and How to Address Them

The plan is simple to describe but harder to carry out. Most internal audit functions will meet some of the following challenges. None of them is a reason to delay; each can be managed if it is recognised early.

Technical Newsletter

Issue 10/2026
(October/2026)

Challenge	Mitigation
Limited capacity. Internal audit teams have limited resources, so adding AI projects to an already full audit plan may delay or replace approved audits.	Include AI work in the annual audit plan presented to the audit committee. State the time required and which audits may be delayed or replaced. Treat AI risk like any other audit risk.
Cost. Certifications, training, enterprise AI tools and co-sourcing all need budget before any visible benefit.	Phase the spending. Start with free or low-cost training for the team, then fund certification for the AI lead. Claim eligible HRD Corp training costs, and link AI spending to regulatory requirements.
Dependence on one person. Once certified, the AI lead becomes attractive to other employers, and the capability can leave with them.	Pair the AI lead with another team member. Document methods, work programmes and lessons learned. Retain skilled staff through options such as certification bonds and clear career paths.

Technical Newsletter

Issue 10/2026
(October/2026)

Challenge

Mitigation

Getting the house in order depends on others. Internal audit can't independently acquire an enterprise AI tool or restrict the use of personal devices and free public tools, and sometimes auditors may hesitate to let go of those free resources.

Agree the approach with IT and the data protection officer. Ensure the team understands client confidentiality and the PDPA. Until an enterprise tool is available, clearly explain what may and may not be entered into public tools.

AI that cannot be seen. There's also the challenge of "shadow AI," which refers to AI features embedded in software that go unnoticed by management. Many won't realise that these are indeed AI functionalities.

Build the inventory from several sources: staff surveys that do not blame, IT network and licence data, and a review of major software contracts and vendor updates. Report the first inventory as a starting point, not a complete list.

No agreed standard to audit against. AI audit standards are still unclear, especially outside finance. There may be no mandatory rules or company policies, so auditors may have to use their own judgement.

Agree the criteria with management before fieldwork: the organisation's own policies, the PDPA, and recognised references such as the National Guidelines on AI Governance and Ethics, ISO/IEC 42001 or the NIST AI Risk Management Framework. Where no framework exists, say so plainly and recommend one.

Technical Newsletter

Issue 10/2026
(October/2026)

Challenge	Mitigation
Protecting independence. Moving from advisory work to assurance over the same arrangements can be questioned under GIAS 2024 if internal audit helped design the framework.	Keep advisory work advisory, with management owning and approving the framework. Document internal audit's role at each stage and disclose earlier advisory involvement to the audit committee. Check co-sourcing providers for any role in selling or implementing the systems under review.
Limited access to vendor AI. Most AI is bought, and vendor contracts rarely give the right to see how a system was trained or tested.	Review vendor contracts during the advisory review and recommend audit and information rights for new and renewed agreements. Until then, rely on the organisation's own controls over the vendor: due diligence, testing before use, monitoring of results and human review.
Board readiness. Board time is limited, and directors may see AI as an IT matter. Without board understanding, assurance cannot be properly questioned.	Keep briefings short, specific to the organisation and built around the questions directors should ask. Link them to directors' own duties, including the duty of care, skill and diligence under Section 213 of the Companies Act 2016 and their personal exposure under the PDPA[12]. Give short, regular updates rather than one long session.

Technical Newsletter

Issue 10/2026
(October/2026)

Challenge	Mitigation
The pace of change. Tools, risks and regulatory expectations can change within months, and early training may be out of date by the later phases.	Review the plan at least once a year and treat it as a living plan. Keep up to date through the IIA, IIA Malaysia and regulators' publications, and share lessons internally.
Knowing whether progress is real. There is no ready measure of AI audit competence, and progress reports can become lists of courses attended.	Assess the team's AI skills against a simple skills matrix at the start and after each phase and co-sourced engagement. Report progress to the audit committee in terms of what the team can now do on its own.

Most of these challenges share a common answer: agree the plan openly with the audit committee, work with management rather than around it, and be honest about what internal audit can and cannot yet assure.

Technical Newsletter

Issue 10/2026 (October/2026)

8. Conclusion

Time is running short, and it's crucial that we get ready. Fortunately, we're starting from a strong place. Our profession has solid skills in things like mapping processes, assessing risks, evaluating IT controls, and providing independent assurance to boards—all of which can easily apply to AI.

However, we're likely to face some challenges along the way. We're dealing with limited capacity and budgets, a reliance on only a few skilled individuals, some hidden AI systems within the organisation, a lack of established standards, the need to maintain independence, and boards that are still getting up to speed on AI. These issues shouldn't slow us down; they can be tackled if we spot and discuss them openly with the audit committee and management early on.

Right now, our focus should be on building our capabilities through structured AI training, developing a clear implementation strategy with the audit committee, and being upfront about what internal audit can and can't guarantee at this stage. Internal auditors who start taking steps now will be in a better position when boards and regulators seek guidance on AI. Those who hesitate might find themselves scrambling when questions arise.

Author: Rosli bin Mohd Rose, CIA, CMIIA

CMIIA Membership No. 002119

Technical Newsletter

Issue 10/2026 (October/2026)

References:

- [1] Bank Negara Malaysia, Artificial Intelligence in the Malaysian Financial Sector, Discussion Paper, 5 August 2025. Based on the BNM AI Survey 2024, 71% of banking institutions and development financial institutions, and 77% of insurers and takaful operators, had implemented at least one AI application in 2024.
- [2] Ibid. More than 60% of banking institutions and of insurers and takaful operators view AI as a strategic priority over the next one to three years.
- [3] Ministry of Science, Technology and Innovation (MOSTI), National Guidelines on AI Governance and Ethics (AIGE), launched 20 September 2024. The guidelines are voluntary.
- [4] See note 1.
- [5] Bank Negara Malaysia, Policy Document on Risk Management in Technology (RMiT), most recently revised on 28 November 2025.
- [6] Personal Data Protection (Amendment) Act 2024 (Act A1727), amending the Personal Data Protection Act 2010 (Act 709). Its provisions came into force in stages on 1 January, 1 April and 1 June 2025.
- [7] Cyber Security Act 2024 (Act 854).
- [8] Companies Act 2016 (Act 777), section 213.
- [9] The Institute of Internal Auditors, Global Internal Audit Standards, published 9 January 2024 and effective 9 January 2025.
- [10] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system; National Institute of Standards and Technology (NIST), Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023.
- [11] The Institute of Internal Auditors, Artificial Intelligence Auditing Framework 2024.
- [12] Personal Data Protection Act 2010 (Act 709), section 133, under which directors and officers may be held personally liable for offences committed by a body corporate.