RDS
ADVOCATES & SOLICITORS

In Business Collaboration:
AMT / ANDERSON MORI & TOMOTSUNE

When AI Joins The Boardroom: Digital Risks & The Fiduciary Duty Of Care

22 September 2026

For more information, please contact:

Michele Kythe Lim (Practice Leader)
michele@rdslawpartners.com

Bahari Yeow Tien Hong
bahari@rdslawpartners.com

David Lee Lai Huat
david.lee@rdslawpartners.com

Tan Sri Datuk Harmindar Singh Dhaliwal
harmindar@rdslawpartners.com

Kamilah Kasim
kamilah@rdslawpartners.com

Rajeswari Karupiah
rajeswari@rdslawpartners.com

S. Saravana Kumar
sara@rdslawpartners.com

For much of modern corporate history, corporate governance in Malaysia was and is built around a relatively straightforward premise: directors are expected to exercise reasonable care in overseeing the affairs of the company. However, the rapid adoption of Artificial Intelligence (AI) is transforming how organisations operate and make decisions. AI now has the potential to significantly enhance the effectiveness of board oversight by improving directors' access to information and analytical capabilities.

As AI becomes embedded in corporate decision-making processes, directors can no longer treat technology governance as a specialist concern. The central governance question is no longer whether organisations should use AI, but whether boards are exercising adequate oversight over the opportunities and risks that AI creates. In this context, the fiduciary duty of care assumes heightened importance as the rise of AI challenges traditional interpretations of this duty. Boards may increasingly rely on systems that they do not fully understand yet remain legally accountable for the outcomes generated by those systems.

The Evolution Of Duty Of Care In The Digital Era

A directors' duty is well codified within the Companies Act 2016 (CA 2016), with Section 213 imposing a fiduciary duty on directors to exercise their powers with reasonable care, skill and diligence, in the best interests of the company. This duty of care requires directors to, *inter alia,* make informed

decisions, actively supervise management and ensure that adequate systems of control exist within the organisation.[1]

With the emergence of AI, they are now increasingly expected to understand not only traditional business risks but also the digital risks associated with technology-enabled decision-making.

These include risks relating to:

- data quality
- algorithmic bias
- cybersecurity vulnerabilities
- confidentiality and data privacy
- model reliability
- governance and regulatory compliance

While the duty of care does not obligate directors to be data scientists or software engineers, it does require sufficient understanding to enable effective oversight and management for AI governance. Directors are not expected to possess deep technical expertise, but they must act with the diligence of an ordinary, prudent person under similar circumstances.

This reflects a broader shift in governance thinking: digital literacy is becoming a governance competency rather than a technical specialisation, and the standard of care is evolving alongside the nature of risk. Consequently, boards that blindly defer to AI outputs without active monitoring will find little shelter under the Business Judgment Rule.

AI As A Governance Risk

Today, many organisations continue to approach AI primarily as a technology initiative, despite AI tools becoming more prevalent in board governance workflows. However, in reality, the increased usage of AI tools in the boardroom now presents governance challenges that extend far beyond technical implementation.

Unlike traditional software, AI can generate outcomes based on large volumes of data that would traditionally have been prepared by management or external advisers. These outputs often influence matters that fall squarely within the board's oversight responsibilities, including financial performance, customer outcomes, regulatory compliance and enterprise risk management. While these capabilities can enhance oversight, they also create two distinct governance risks:[2]

[1] Section 213 of the Companies Act 2016; Malaysian Code of Corporate Governance (Practice 10.1)
[2] Page 5, Using AI in the boardroom—new opportunities and challenges, PwC

1. Board overreach:

   Directors using AI to analyse independent information could invite boards to step over the oversight boundary and engage in functions that should be driven by management

2. Overreliance:

   The apparent objectivity of AI-generated outputs may lead directors to place blind faith in outputs which may be "hallucinated".

AI has the potential to provide directors with unprecedented access to operational data. While this may appear beneficial, it blurs the distinction between oversight and management and may tempt directors to become involved in day-to-day decision-making, second-guess management decisions or intervene in matters that properly fall within management's remit. Such involvement risks undermining accountability, as management cannot be held responsible for decisions if the board increasingly assumes operational functions.

Moreover, there is a risk that boards begin to treat AI-generated recommendations as authoritative rather than advisory, known as automation bias. Such reliance by directors is likely to fall outside the statutory safeguards provided under Section 215 of the CA 2016. This provision affords directors a degree of protection only when they rely, in good faith, on information and advice prepared by certain qualified groups of people. As AI tools are neither legal persons capable of being held accountable nor subject to professional standards, fiduciary obligations or duties of care,[3] deferring to an algorithm therefore creates a gap in liability that leaves directors legally exposed.

The governance challenge, therefore, is whether boards can harness AI's capabilities without compromising the fundamental principles of accountability, independence and proper role delineation. In an AI-enabled environment, the most effective boards will be those that resist the temptation to trust technology unquestioningly and the ability to manage through it.

The New Foundations Of Oversight: Data Governance And Cybersecurity

AI cannot be separated from data and technology governance.

The effectiveness of AI systems depends fundamentally on the quality, integrity and security of underlying data. Consequently, weaknesses in data management can rapidly become governance failures. This is particularly relevant in Malaysia, where organisations operate within an increasingly complex regulatory environment involving personal data protection, cybersecurity obligations and digital risk management requirements, especially in light of the proposed AI Governance Bill and the upcoming

[3] AI in the Boardroom: Governance Implications and Fiduciary Considerations, David Chriki, David A. Gordon, Holly J. Gregory, Andrea L. Reed

revision to the Securities Commission's (SC) Malaysian Code on Corporate Governance (MCCG).

In the proposed enhancements to the MCCG, the SC recognised the transformative role of AI as an integral part of technology governance by proposing a more proactive approach to technology governance. Boards are now expected to oversee both the risks and strategic opportunities arising from technology adoption, which includes ensuring appropriate governance structures, maintaining accountability for technology-related decisions, overseeing risks relating to cybersecurity, data governance, privacy and operational resilience, as well as maintaining sufficient technology literacy to effectively discharge their oversight responsibilities.[4]

Recent cyber incidents across both the public and private sectors have further affirmed that technology failures can rapidly become board-level crises. Infamously the CrowdStrike incident which began as a mere faulty software update, has since escalated to a global outage, putting an immediate halt to many organizations' operations and resulting in a global loss of approximately $5.4 billion.[5] This only demonstrates that the increasing adoption of technologies such as AI only reinforces the need for stronger oversight of digital and technological risks.

Building An AI Governance Framework

As AI adoption accelerates, boards should consider whether existing governance structures remain fit for purpose, especially when reviewing the effectiveness of their risk management and internal control framework pursuant to Practice 10.1 of the MCCG.

Effective AI governance does not necessarily require the creation of entirely new frameworks. Rather, it requires integrating AI-related risks into existing governance and risk management structures. Recognising this, this is now reflected in relatively recent changes to corporate regulation and compliance with the Securities Commission's Guidelines on Technology Risk Management (TRM Guidelines) effected on 19 August 2024, as well as the Statement on Risk Management and Internal Control Guidelines 2025 (SORMIC Guidelines 2025).

Chapter 5 of the TRM Guidelines requires the board to provide oversight and accord sufficient priority and resources to manage technology risk, as part of the overall risk management framework of a capital market entity.

In addition, an AI-accelerated board is required to adopt the 'Guiding Principles Relating to the Adoption of Artificial Intelligence (AI) and Machine Learning (ML)', specified in Appendix 3 of the TRM Guidelines, which are guided by the following principles:

[4] Section 3, Public Consultation Paper No. 1/2026, Proposals to Strengthen Corporate Governance Ecosystem, Securities Commission Malaysia
[5] https://sps.columbia.edu/news/crowdstrike-crisis-anatomy-digital-catastrophe

- Accountability;
- Transparency;
- Fairness and non-discrimination; and
- Practical accuracy and reliability.

The SORMIC Guidelines 2025 on the other hand is a governance guidance document aimed to facilitate boards of listed companies in preparing the mandatory Statement on Risk Management and Internal Control (SORMIC) required under Paragraph 15.26(b) of Bursa Malaysia's Listing Requirements.

Amending an earlier 2012 governance guidance that focused largely on traditional financial and operational risks, the SORMIC Guidelines 2025 reinforces the expectation that boards should adopt a forward-looking approach to risk management by recognising that technology risks should be embedded within the Board's oversight processes.[6]

The addition of Appendix I of the SORMIC Guidelines 2025 further identifies AI, cyber security and technology risks as an important emerging global risk that organisations should assess. Together with the TRM Guidelines, the SORMIC Guidelines 2025 reflects an emerging regulatory expectation that technology governance is part of the board's fiduciary responsibilities, rather than just another operational risk.

Other practical measures to ensure an effective framework may also include:[7]

- Formally including AI in boardroom discussions
- Commit to upskilling directors' AI literacy
- Enable secure AI use within a company-approved environment
- Maintain human oversight
- Prepare for investor transparency
- Identify accountability for AI governance at both management and board levels

These measures are further enhanced and operationalized through the Boardroom Primer for AI Adoption & Governance, published by our National AI Office. Despite not being binding in nature, the Primer sets out a five-stage implementation framework for adopting AI systems responsibly and effectively. At the planning stage, this means testing whether a proposed use case genuinely requires an AI solution and confirming the organisation holds the legal rights and data governance arrangements needed to use the underlying data. When pairing with a vendor, boards should then interrogate dependencies, data provenance and exit options before committing. Before any deployment is scaled, they should confirm organisational readiness, including workforce impact and change management, and before systems go live, they should require independent or third-party validation rather than technical accuracy testing alone. Once deployed, boards should set clear thresholds for human intervention, incident escalation and eventual decommissioning. Applied consistently across these

[6] Section 4.8, Statement on Risk Management and Internal Control Guidelines 2025
[7] Page 7, Using AI in the boardroom—new opportunities and challenges, PwC; AI in the Boardroom: Governance Implications and Fiduciary Considerations

stages, this approach converts AI governance from a one-off approval into an ongoing discipline that is revisited as systems change in purpose, scale, data, users, context or legal obligations, giving directors a defensible record of the enquiries made at each stage in discharging their duty of care.

The objective is not to eliminate all AI-related risks. Instead, it is to ensure that AI adoption remains consistent with the organisation's risk appetite, governance standards and stakeholder expectations, supported by a structured, staged approach to adoption.

Conclusion

The increasing presence of AI in corporate decision-making represents one of the most significant governance developments facing Malaysian boards today. Yet the fundamental principles of governance remain unchanged. Directors continue to owe duties of care, remaining responsible for overseeing risk and exercising independent judgment in the best interests of the company.

What has changed is the nature of the risks that boards must understand and manage. In the same way that cybersecurity and sustainability evolved from operational concerns into governance priorities, AI is now making a similar transition. Boards that fail to engage with these developments may find themselves exposed to legal, operational and reputational risks that traditional governance frameworks were not designed to address.

Ultimately, AI may transform how information is generated, analysed and presented to directors. It does not, however, alter the central principle upon which governance rests: accountability remains human.

This publication is for educational and informational purposes only and is not intended and should not be construed as legal advice.

KUALA LUMPUR
Level 16, Menara 1 Dutamas No. 1, Jalan Dutamas 1, Solaris Dutamas, 50480 Kuala Lumpur
T: +603 6209 5400
F: +603 6209 5411
enquiry@rdslawpartners.com

PENANG
Suite S-21E & F21st Floor, Menara Northam, No. 55, Jalan Sultan Ahmad Shah, 10050 Penang
T: +604 370 1122
F: +604 370 5678
generalpg@rdslawpartners.com

JOHOR BAHRU
8-35, Menara Delima Satu, Jalan Forest City 1, Pulau Satu, 81550 Gelang Patah, Johor Bahru
T: +607 585 6414
F: +607 509 7614
generaljb@rdslawpartners.com