

AI Governance Made Practical: Global Standards with Local Flavour

將全球標準結合本地特色可實現人工智能企業管治

Edwin Bernard

Hong Kong continues to solidify its position as a premier global hub for technology and innovation, recently climbing to 4th place in the IMD World Digital Competitiveness Ranking (WDCR) 2025. This leadership was further validated by the United Nations' "Technology and Innovation Report 2025: Inclusive Artificial Intelligence for Development," published on December 19, 2025. Evaluating over 100 economies, the report identifies Hong Kong as a global leader in AI readiness, awarding it the highest rating in all three critical pillars: infrastructure, data, and skills.

As Artificial Intelligence moves from the "experimental" phase into the core of corporate operations, the burden of oversight has shifted squarely to the Boardroom. For Hong Kong Directors, the challenge is no longer just "if" to adopt AI, but "how" to govern it amidst a complex web of global standards and local expectations.

While Hong Kong's regulatory bodies provide essential high-level principles—focusing on accountability, transparency, and fairness—they do not prescribe a specific

operational "how-to" manual. To bridge this gap, boards should look to the NIST AI Risk Management Framework (NIST AI RMF) and ISO/IEC 42001, the two preeminent global frameworks defining how organisations design, deploy, and monitor AI responsibly. Yet, Directors must remain vigilant; while these international standards are world-class, they must be infused with a "local flavour" to meet Hong Kong's unique regulatory requirements.

NIST AI RMF: The Toolkit

The NIST AI RMF is a globally recognised toolkit used to build and deploy artificial intelligence safely. It addresses AI-specific challenges such as algorithmic bias, hallucinations, and system transparency. The toolkit is built around four core functions: Govern (setting the rules), Map (identifying specific risks), Measure (testing performance), and Manage (day-to-day oversight).



For Board members, the NIST toolkit acts as a strategic bridge that turns technical complexity into manageable business risk:

- **Fiduciary Oversight:** It provides a "common language" for Directors to communicate with technical teams, ensuring AI risk is managed as a core business liability rather than an isolated IT issue.
- **Regulatory Compliance:** While voluntary, this toolkit aligns with global laws (such as the EU AI Act) and local guidelines (like those from Hong Kong's PCPD), helping the Board shield the company from legal and reputational damage.
- **Informed Decision-Making:** The toolkit mandates evidence-based reporting—such as bias audits and error rates—giving Directors the tangible data they need to approve AI investments with confidence.
- **Building Market Trust:** Using the NIST toolkit signals to investors and customers that the organisation is a responsible steward of technology, thereby protecting the brand's long-term value and "license to operate."

Major global corporations and professional services firms—including JPMorgan Chase, Microsoft, Google, IBM, and the "Big Four" consultancy firms—utilise the NIST AI RMF as the gold standard for managing AI risk and building trustworthy systems. The framework is free and publicly available via the NIST website.

ISO/IEC 42001: The Certificate



ISO/IEC 42001 is the world's first certifiable standard for an Artificial Intelligence Management System (AIMS). It is applicable across all industries and relevant for public sector agencies as well as companies or non-profits.

Implementing this standard offers significant benefits centred on risk management, regulatory compliance, and gaining a competitive advantage.

Unlike the NIST framework, ISO/IEC 42001 allows a company to achieve formal certification via accredited third-party auditors—a process that involves a financial investment. Certification is increasingly becoming a prerequisite for international procurement, proving to stakeholders that an organisation has a verifiable, repeatable system for managing AI.

For a Director, its primary value lies in its ability to treat AI as

a core enterprise function rather than a siloed IT project. The standard requires the Board to define a formal AI policy and assign clear roles and responsibilities. This ensures that accountability for AI outputs rests with senior leadership, providing the clear chain of command that local authorities expect from licensed corporations.

Adoption is already visible among global leaders. Google obtained certification for its Cloud services, while KPMG was among the first of the "Big Four" to attain ISO/IEC 42001 certification. Locally, Hong Kong-headquartered DYXnet, an AI+ Cloud-Network-Security service provider, was one of the first ICT service providers in the region to obtain this certification in July 2025.

Local Flavour

International frameworks like the NIST AI RMF and ISO/IEC 42001 are not "plug-and-play" solutions for Hong Kong. In the HKSAR's sector-led regulatory environment, increasingly coordinated by the Digital Policy Office (DPO), international standards may serve as a baseline but should be synchronised with local statutory mandates.

Boards must ensure their teams customise international frameworks to address Hong Kong's statutory and sector-specific requirements:

- **Personal Data Privacy:** Compliance with ISO or NIST does not equate to compliance with Hong Kong's Personal Data (Privacy) Ordinance (PDPO). To provide a clear local roadmap, the Office of the Privacy Commissioner for Personal Data (PCPD) issued the "Guidance on the Ethical Development and Use of Artificial Intelligence" and the "Artificial Intelligence: Model Personal Data Protection Framework" (2024). Organisations should embrace three fundamental values: being respectful, beneficial, and fair to stakeholders. Top management is expected to formulate a clear (ethical) AI strategy and establish an AI Governance Committee with sufficient authority and expertise to oversee the entire AI lifecycle, including the procurement of third-party solutions.
- **Financial Sector Accountability:** The SFC explicitly links AI governance to senior management responsibilities, mandating that Managers-in-Charge (MICs) and senior management ensure effective policies and internal controls are in place throughout an AI model's lifecycle. Similarly, the HKMA has established guiding principles for Big Data and AI (BDAI) focusing on four major areas: (1) governance and accountability, (2) fairness, (3) transparency and disclosure, and (4) data privacy and

protection. The HKMA holds the board and senior management accountable for AI-driven decisions and expects specific "Human-in-the-Loop" safeguards that are often more prescriptive than general international guidelines.

- **Healthcare & Medical Requirements:** Organisations deploying AI in healthcare must align with the Department of Health's Technical Reference TR-008: "Artificial Intelligence Medical Devices (AI-MD)". It provides clarity for devices using AI and machine learning, including Continuous Learning Capability (CLC) and the technical requirements expected for listing these devices on the Medical Device Administrative Control System (MDACS). This ensures that AI-driven medical devices meet local clinical safety and administrative control requirements before being listed for use in the HKSAR.

Strategic Advantages

Successfully integrating international frameworks with Hong Kong regulations offers three distinct advantages:

1. **Regulatory Future-Proofing:** By adopting these standards now, companies position themselves ahead of potential future binding legislation. A firm already aligned with ISO and NIST will find any transition to new laws and regulatory guidance far more seamless.
2. **Global Interoperability:** For Hong Kong-listed companies with global operations, these standards allow for a "build once, comply everywhere" approach, navigating the reach of foreign laws like the EU AI Act.
3. **Maintaining Digital Leadership:** Robust, localised governance ensures that AI innovation does not lead to reputational setbacks. As Hong Kong cements its status as a global digital hub, Boards that bridge the gap between global standards and local rules will be the ones to secure long-term market trust.

Conclusion

In 2026, AI governance is no longer a "tech issue" but a core fiduciary duty that demands board-level attention. While the NIST toolkit and ISO certification provide world-class foundations, their true value in Hong Kong is unlocked only when localised to meet our unique sectoral guardrails. By bridging the gap between international best practices and Hong Kong's specific regulatory expectations, Directors do more than just ensure compliance; they build a foundation of trust that protects their organisation's reputation and secures its place at the forefront of the city's digital future. 

Edwin Bernard - MSc, CEFA, CAITL (Certified Artificial Intelligence Transformation Leader, USAII), Hong Kong, January 2026.

香

港一直努力不懈鞏固作為全球重要技術和創新樞紐的地位，在「2025年世界數碼競爭力排名」中攀升至第四位。聯合國於2025年12月19日發表的《2025年技術和創新報告：包容性人工智能促進發展》進一步印證香港在這方面領先。該報告評估超過100個經濟體，認定香港在人工智能準備程度方面領先全球，故在「基建」、「數據」和「技能」三大關鍵支柱的排名上將香港列於首位。

隨著人工智能從「實驗」階段進入企業營運的核心，監管重任已全然交給董事會會議。香港董事面對的挑戰不再只是「假如」採用人工智能會怎樣，而是「如何」在交織著各種全球標準和本地預期的複雜情況下管治企業。

雖然香港規管機構提供必要的高層次原則（以問責、透明度和公平為重點），但並無提供明確的營運「操作」指引。為彌補這點不足，企業董事會應該參考國家標準技術研究所的《人工智能風險管理框架》（NIST AI RMF）和ISO/IEC 42001。這兩項重要的全球框架說明機構如何負責任地設計、調配和監督人工智能。但是，董事必須保持警覺，因為儘管這些國際標準屬世界級，但必須跟「本地特色」融匯貫通才能符合香港獨特的監管規定。

人工智能風險管理框架：工具套件

NIST AI RMF是全球認同的工具套件，供安全打造和調配人工智能，特別針對種種人工智能挑戰，例如演算法偏誤、幻覺和系統透明度。這個工具套件以四個核心功能為重點：管治（訂定規則）、寫像（確定風險）、測量（測試表現）和管理（日常監督）。對董事會成員來說，國家標準技術研究所的這個工具套件將複雜技術化為可以管控的商業風險：

- **受委託監督：**框架為董事提供「共通語言」方便跟技術團隊溝通，確保可將人工智能風險成為核心企業責任而非個別資訊科技問題。
- **合規：**這個工具套件雖是自發制定但配合全球法例（例如《歐盟人工智能法案》）和當地指引（例如香港個人資料私隱專員公署發佈的指引），有助董事會避免觸犯法例和聲譽受損。
- **知情決定：**這個工具套件規定作循證匯報（例如偏見審計和錯誤率），為董事提供有信心批准人工智能投資所需的實質數據。

- 建立市場信任：採用國家標準技術研究所的這個工具套件可向投資者和客戶顯示企業負責善管理科技，從而保護品牌的長遠價值和「經營特許」。

多間主要的全球企業和專業服務公司均以NIST AI RMF作為管控人工智能風險和建立信任制度的黃金標準，包括摩根大通、微軟、Google、IBM和「四大」會計師行。這個框架是公開的，可在國家標準技術研究所的網站免費下載。

ISO/IEC 42001：認證

ISO/IEC 42001是全球首個人工智能管理制度認證標準，適用於所有行業、公營機構、商企和非牟利機構。執行此標準對風險管理和合規有莫大裨益，還可加強競爭優勢。

有別於國家標準技術研究所的框架，ISO/IEC 42001容許公司透過認可的第三方審計師正式認證——當中涉及財務投資。認證已日益成為國際採購的必要先決條件，向持份者證明機構有可驗證、可重覆的人工智能管控制度。

對董事來說，其主要價值在於能夠將人工智能作為核心企業功能而非孤立的人工智能項目。根據這項標準，董事會必須制定正式的人工智能政策和明確分配崗位和責任，以確保高層領導人員為人工智能輸出問責，以及提供當地規管當局預期特許企業會提供的明確指揮鏈。

多間全球領先企業均已採用。Google已為其雲端服務取得認證，畢馬威是「四大」之中率先獲得ISO/IEC 42001認證的一間。本地方面，總部設於香港的人工智能和雲端網絡安全服務供應商DYXnet於2025年7月取得此認證，是區內率先獲此認證的資訊與通訊科技服務供應商之一。

本地特色

對香港來說，NIST AI RMF和ISO/IEC 42001一類國際框架並非「即插即用式」解決方案。香港特別行政區的規管屬行業主導，而且數碼政策辦公室日益加強統籌，各項國際標準雖然可以充當底線，但必須跟本地的法定指令同步配合。

董事會必須確保團隊按情況調整國際框架，以配合香港的法定規定和行業要求：

- 個人資料私隱：遵從ISO或NIST並不等於遵從香港的《個人資料（私隱）條例》。為提供清晰的本地路線圖，個人資料私隱專員公署發佈了《開發及使用人工智能道德標準指引》和《人工智能：個人資料保障模範框架》（2024年）。各企業應該緊守三項基本價值觀：尊重持份者、惠及持份者和公平對待持份者。最高級管理

層應該制定（符合道德的）清晰人工智能策略和成立人工智能管治委員會。委員會應獲賦予充分權限和具備專業知識，在人工智能的整個生命周期加以監督，包括採購第三方解決方案。

- 金融界的問責性：證監會將人工智能管治跟高層管理人員的責任明確掛鉤，規定核心職能主管和高級管理層必須確保在人工智能模型的整個生命周期實施有效的政策和內部監控措施。同樣，金管局也有為大數據分析和人工智能（BDAI）制定指導原則，四大範疇包括：(1) 管治與問責、(2) 公平性、(3) 透明度與披露以及 (4) 資料私隱與保障。金管局認為董事會和高級管理層必須為以人工智能作出的決定負責，並且預期採用某些「人在環中」預防措施，這類措施往往更勝一般的國際指引。
- 健康護理與醫療規定：採用人工智能提供健康護理的機構必須遵從衛生署的技術參考文件TR-008：《人工智能醫療器械》（AI-MD）。該文件清楚界定使用人工智能和機器學習的器械，包括持續學習能力（CLC）以及醫療器械行政管理制度（MDACS）的表列技術要求，以確保人工智能驅動的醫療器械表列用於香港特別行政區之前已符合本地的臨床安全和行政管理要求。

策略優勢

成功將國際框架整合香港的法例有三大優勢：

1. 配合未來規管：企業現在採用這些標準等於為應對未來的法例約束作預先部署。已遵從ISO和NIST的公司可以遠較未配合的公司更順利過渡至新法例和規管指引。
2. 全球互用性：對於在全球營運的香港上市公司來說，這些標準讓公司可以做到「一次構建、到處合規」，能夠配合《歐盟人工智能法案》等外國法例。
3. 保持數碼領導地位：卓越的本地化企業管治可確保人工智能創新不令信譽受挫。隨著香港致力鞏固作為全球數碼樞紐的地位，能夠彌合全球標準和本地規則隔閡的董事會，定必獲得長久的市場信任。

結論

在2026年，人工智能企業管治不再是「技術問題」，而是需要董事會層面處理的核心受託責任。雖然國家標準技術研究所的工具套件和ISO認證提供世界級基礎，但要釋放出其在香港的真正價值，必須將之本地化以符合香港獨特的行業護軌。如果董事會能彌合國際最佳實務和香港規管預期之間的隔閡，不單止能確保合規，還能打造基礎以保護所屬機構的聲譽和在香港的數碼未來穩守前緣。

Edwin Bernard，MSc、CEFA、CAITL（美國人工智能研究所認可人工智能革變領袖）

The 21st Century DIRECTOR

廿一世紀
董事

Publisher 出版機構

The Hong Kong Institute of Directors 香港董事學會

Sponsor 贊助機構

Corporate Governance Development Foundation Fund 企業管治發展基金

Publishing Board 出版委員會

Mr Stanley Mok (Chairman) 莫兆光先生 (主席)
Ms Bonnie S Y Chan 陳心愉女士
Prof Agnes K Y Tai 戴潔瑩教授
Mr Jonathan Shea 謝達安先生
Mr Richard Tsang 曾立基先生

Project Management 項目統籌

Secretariat, The Hong Kong Institute of Directors
香港董事學會秘書處

For enquiries about circulation and advertisement, please contact:

有關發行及廣告查詢，請聯絡：

Chief Business Officer & Head of Training: Ms Miriam Yee

業務總監及培訓主管：余海恩小姐

For editorial enquiries, please contact:

有關編輯上的查詢，請聯絡：

Associate Manager, Communication & Projects: Mr Wing Wong

傳訊及項目助理經理：王俊泳先生

Tel 電話：+852 2889 1414

Fax 傳真：+852 2889 9982

Email 電郵：magazine@hkiod.com

《廿一世紀董事》同時可於網上閱覽

The 21st Century Director is also available at

<https://www.hkiod.com/21st-century/>

ISSN 1996-9619

Sponsored by 贊助機構：

Corporate Governance
Development Foundation Fund
企業管治發展基金



The Hong Kong Institute of Directors 香港董事學會

Patron 贊助人

The Hon John LEE Ka-chiu GBM SBS PDSM PMSM 李家超行政長官

Founder Chairman & Hon President 創會主席兼榮譽會長

Dr the Hon Moses Cheng GBM GBS OBE JP 鄭慕智博士

Past Chairmen 前任主席

Dr Herbert H M Hui JP (Deceased) 許浩明博士 (已故)

Mr Peter S H Wong MBA 黃紹開先生

Dr Kelvin Wong SBS JP DBA 黃天祐博士

Mr Henry Lai 賴顯榮律師

Dr Christopher To 陶榮博士

Council 理事會 (2025-2026)

Chairman 主席：

Mr Richard Tsang 曾立基先生

Deputy Chairmen 副主席：

Ir Edmund K H Leung SBS OBE JP 梁廣灝工程師

Ms Bonnie S Y Chan JP 陳心愉女士

Mr William Lo 羅志聰先生

Ms Alice Yip 葉嘉明女士

Treasurer 司庫：

Mr Vincent Chan MH 陳永誠先生

Immediate Past Chairman 卸任主席：

Dr Christopher To 陶榮博士

Chief Executive Officer 行政總裁：

Mr Jonathan Shea 謝達安先生

Council Members 理事會成員：

Mr Clement Kam Wing Chan 陳錦榮先生

Dr Leonard S K Chan 陳新國博士

Mr Hamilton Cheng 鄭炳熙先生

Prof Anthony Cheung 張振宇教授

Mr Richard Ho 何麗康先生

Mr Randy Hung 孔敬權先生

Mr Ip Shing Hing BBS JP 葉成慶律師

Dr Alan Lai 黎嘉豪博士

Mr Henry Lai 賴顯榮律師

Mrs Margaret S Leung 梁甘秀玲女士

Mr Ka-Yin Li 李家彥先生

Mr Jeffrey Mak 麥振興律師

Mr Man Mo Leung 文暮良先生

Ir Prof John Mok 莫建輝教授

Mr Stanley Mok 莫兆光先生

Ms Athena Y W Ng 吳溢穎女士

Prof Agnes K Y Tai 戴潔瑩教授

Mr Jim Wardell 詹華達先生

Mr Stephen Weatherseed 韋大象先生

Mr Andrew Weir BBS JP 韋安祖先生

Mr Kenneth Wong 黃永恩律師

Advisory Board 顧問委員會：

Dr Justin K H Chiu 趙國雄博士

Dr David Wong GBS JP 黃友嘉博士

Mr Huen Wong SBS BBS JP 王桂壠律師

Dr Samuel Yung GBS SBS MH JP 容永祺博士

Dr Carlye Tsui SBS MBE JP 徐尉玲博士

The 21st Century Director is the official magazine of The Hong Kong Institute of Directors. All rights reserved. No part of this magazine may be reproduced or stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of the publisher and/or the copyright owner of this magazine. Quotation of short passages of the magazine for the purposes of review and education is allowed provided that it is made with explicit reference to the source and publisher. Neither the magazine nor the publisher accepts liability for any views, opinions or advice expressed by writers and interviewees of articles. The contents of the magazine do not necessarily reflect the views or opinions of The Hong Kong Institute of Directors or the members of the Institute and no liability is accepted in relation thereto. This magazine includes articles that have been invited from or contributed by authors. While such articles present the views of the respective authors, these articles may not necessarily represent the views of the Publishing Board of the magazine or The Hong Kong Institute of Directors. It is the intention of the Institute to present views from various perspectives, which may inspire thinking and generate constructive discussions.

《廿一世紀董事》是香港董事學會的官方雜誌。本雜誌所有出版內容的版權為香港董事學會所有。未經出版人及 / 或版權擁有人書面同意，本雜誌所有內容一律不得以任何形式或以任何工具（電子、機械、影印、錄製或其它工具）翻印、儲存或引進於檢索系統或傳送。本雜誌內容可供摘要引述以作研討或教育用途，但必須註明出處或出版人。本雜誌及出版機構不會為雜誌內作者及被訪者所表達的觀點、意見或建議負責任。雜誌的內容並不一定反映香港董事學會或學會會員的觀點及意見，學會與會員均不因此而負上任何責任。本雜誌收錄邀約作者及供稿作者的文章，然而這些文章表達了其作者的觀點，卻不一定代表雜誌出版委員會或香港董事學會的觀點。學會的用意是容納多角度的意見，這或可啟發思考及產生具建設性的討論。

© The Hong Kong Institute of Directors 香港董事學會 © 版權所有

The Hong Kong Institute of Directors is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors.

香港董事學會為香港代表專業董事的首要組織，其宗旨是促進所有公司的持久成就；為達成使命，學會致力提倡優秀企業管治與釐訂相關標準，以及協助董事的專業發展。

The Hong Kong Institute of Directors Executive Office 香港董事學會行政處

2104 Shanghai Industrial Investment Building, 48 Hennessy Road, Wan Chai, Hong Kong 香港灣仔軒尼詩道48號上海實業大廈2104

Tel 電話：(852) 2889 9986 Fax 傳真：(852) 2889 9982 E-mail 電郵：executive@hkiod.com



The Hong Kong Institute of Directors 香港董事學會



The Hong Kong Institute of Directors