CGj

November 2025

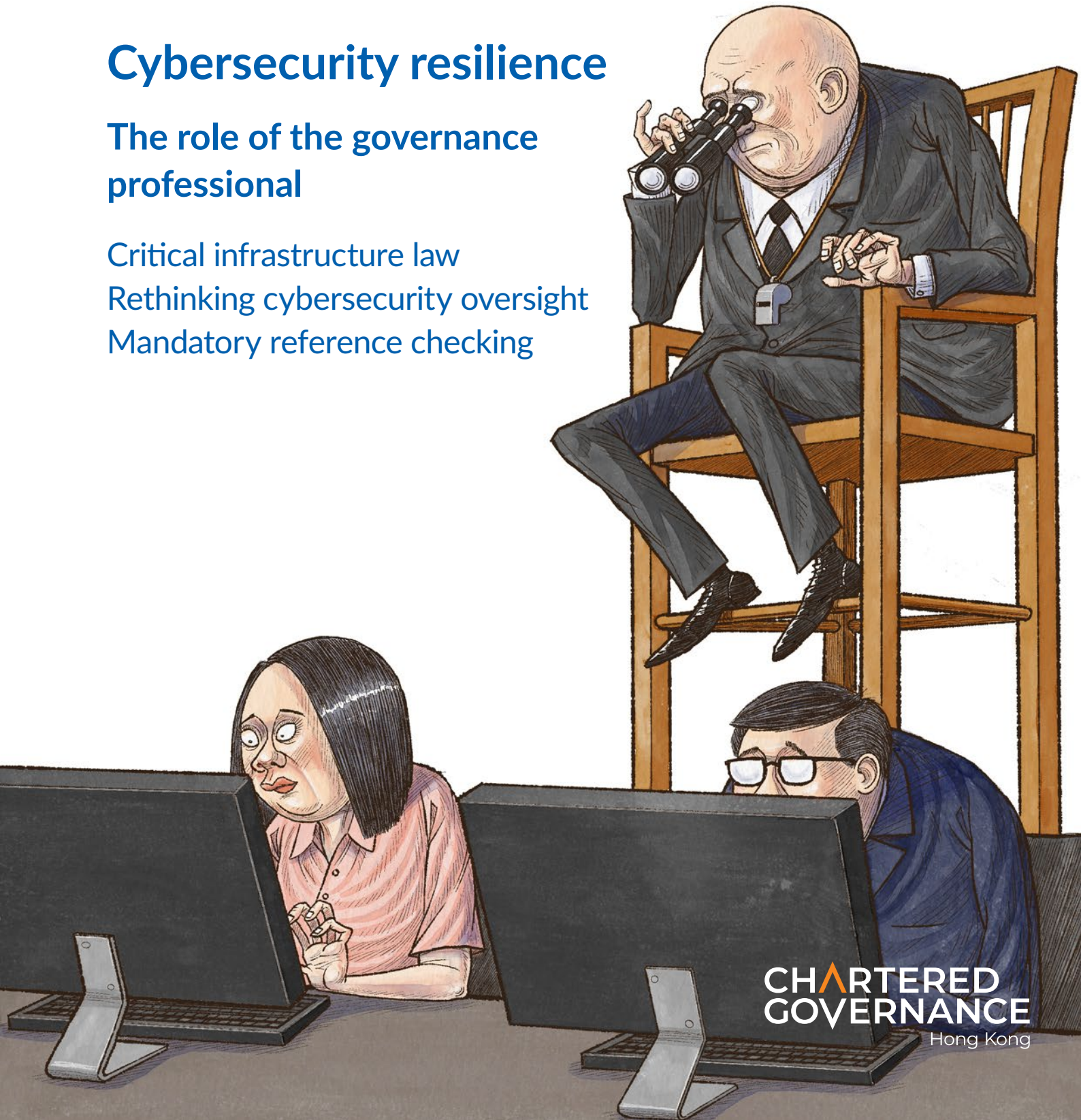
Better Governance.
Better Future.
卓越治理 更佳未來

The journal of the Hong Kong
Chartered Governance Institute
香港公司治理公會會刊

Cybersecurity resilience

The role of the governance professional

Critical infrastructure law
Rethinking cybersecurity oversight
Mandatory reference checking



CHARTERED GOVERNANCE
Hong Kong

CHARTERED GOVERNANCE
Hong Kong

HKCGI Director Training Package

A Complete Solution

Competitive Pricing for Companies

40 units HK$13,800 only

60 units HK$20,100 only

New HKEX CG Code effective 1 July 2025—are your directors prepared?

A multilingual package featuring industry-leading experts, the **Director Training Package** is a flexible, cost-effective solution for meeting HKEX's new regulatory requirements.

What Differentiates Us

- **RECOGNISED TRAINING PROVIDER COVERING ALL 5 HKEX-MANDATED TOPICS**
- **ON-DEMAND VIDEO ACCESS FOR SELF-PACED LEARNING**
- **CENTRALISED RECORD-KEEPING TO STREAMLINE COMPLIANCE REPORTING**
- **A CERTIFICATE OF COMPLETION & INSTITUTE-RECOGNISED CPD HOURS**

Hear from the Experts

DAVID SIMMONDS
FCG HKFCG
Chief Strategy, Sustainability & Governance Officer, CLP Holdings Limited; President, HKCGI

HKCGI's Director Training Package represents exactly what boards need today—comprehensive, flexible training that aligns with HKEX requirements.

EDITH SHIH
FCG(CS, CGP) HKFCG(CS, CGP)(PE)
Executive Director & Company Secretary, CK Hutchison Holdings Limited; Past International President, CGI; Honorary Adviser to Council & Past President, HKCGI

As an executive director, I know HKCGI's training is top notch. I recommend this to directors and those facilitating training for them.

GILL MELLER
FCG HKFCG(PE)
Legal and Governance Director, MTR Corporation Limited; International Vice President, CGI; Past President, HKCGI

HKCGI's Director Training Package balances regulatory compliance with practical flexibility. This is the kind of forward-thinking solution boards need.

For more information, contact HKCGI's Professional Development Section

+852 2881 6177 cpd@hkcgi.org.hk www.hkcgi.org.hk

CHARTERED GOVERNANCE
Hong Kong

HKCGI Foundation
Scholarships and Subject Prizes

The HKCGI Foundation will allocate a total of **HK$280,000** to local universities for the **2025/2026 academic year**.

This will recognise students with outstanding academic performances in governance-related disciplines.

23 Scholarships

38 Subject Prizes

Nurturing the next generation of governance professionals!

Partnering Universities:

- City University of Hong Kong
- Hong Kong Metropolitan University
- Lingnan University
- The Chinese University of Hong Kong
- The Hong Kong Polytechnic University
- The University of Hong Kong
- Hong Kong Baptist University
- Hong Kong Shue Yan University
- Saint Francis University
- The Hang Seng University of Hong Kong
- The Hong Kong University of Science and Technology

Key benefits:

- Fast-track your journey towards earning HKCGI professional qualifications
- Gain a competitive advantage for your career in corporate governance
- Obtain access to a network of governance professionals

Application:

For details, visit your university's scholarship website or contact the student office.

*Note: Selection is merit-based and conducted by the university.

CGj

CHARTERED GOVERNANCE Hong Kong

Good governance comes with membership

About The Hong Kong Chartered Governance Institute

The Hong Kong Chartered Governance Institute (HKCGI, the Institute) is an independent professional body dedicated to the promotion of its members' role in the formulation and effective implementation of good governance policies, as well as the development of the profession of the Chartered Secretary and Chartered Governance Professional in Hong Kong and the Chinese mainland.

The Institute was first established in 1949 as an association of Hong Kong members of The Chartered Governance Institute (CGI). In 1994 the Institute became CGI's Hong Kong Division and, since 2005, has been CGI's Hong Kong/China Division.

The Institute is a founder member of Corporate Secretaries International Association Ltd (CSIA), which was established in March 2010 in Geneva, Switzerland. Relocated to Hong Kong in 2017, where it operates as a company limited by guarantee, CSIA aims to give a global voice to corporate secretaries and governance professionals.

HKCGI has about 10,000 members, graduates and students.

Membership and studentship statistics update

As of 30 September 2025, the statistics were as follows:
Students: 2,259 **Graduates**: 420 **Associates**: 6,593 **Fellows:** 942

The Hong Kong Chartered Governance Institute

(Incorporated in Hong Kong with limited liability by guarantee)
3/F, Hong Kong Diamond Exchange Building,
8 Duddell Street, Central, Hong Kong
Tel: (852) 2881 6177 Fax: (852) 2881 5050
Email: ask@hkcgi.org.hk (general)
cpd@hkcgi.org.hk (professional development)
member@hkcgi.org.hk (member)
student@hkcgi.org.hk (student)
Website: www.hkcgi.org.hk

Beijing Representative Office

Room 1220, Jinyu Tower,
No 129, Xuanwumen West Street,
Xicheng District, Beijing, 100031, PRC
Tel: (86) 10 6641 9368/6641 9190
Email: bro@hkcgi.org.hk
Website: www.hkcgi.org.cn

The Chartered Governance Institute

The Chartered Governance Institute
CGI Global
Saffron House
6–10 Kirby Street
London EC1N 8TS
United Kingdom
Tel: (44) 1730 715 226

Governance Institute of Australia
Level 11, 10 Carrington Street
Sydney, NSW 2000
Australia
Tel: 1800 251 849

The Chartered Governance Institute of Canada
1568 Merivale Road, Suite 739
Ottawa, ON Canada K2G 5Y7
Tel: (1) 613 595 1151
Fax: (1) 613 595 1155

MAICSA
No 57 The Boulevard
Mid Valley City
Lingkaran Syed Putra
59200 Kuala Lumpur
Malaysia
Tel: (60) 3 2282 9276
Fax: (60) 3 2282 9281

Governance New Zealand
PO Box 444
Shortland Street
Auckland 1140
New Zealand
Tel: (64) 9 377 0130

SAICSA
149 Rochor Road
#04–05 Fu Lu Shou Complex
Singapore 188425
Tel: (65) 6334 4302
Fax: (65) 6334 4669

Chartered Governance Institute of Southern Africa
PO Box 3146
Houghton 2041
Republic of South Africa
Tel: (27) 11 551 4000
Fax: (27) 11 551 4027

The Chartered Governance Institute UK & Ireland
Saffron House, 6–10 Kirby Street
London EC1N 8TS
United Kingdom
Tel: (44) 20 7580 4741

Chartered Governance and Accountancy Institute in Zimbabwe
Cnr 3rd St & Nelson Mandela
PO Box 2417
Zimbabwe
Tel: (263) 242 707582/3/5/6

November 2025

CGj, the journal of the Institute, is published 12 times a year by Ninehills Media and is sent to members and students of the Institute and to certain senior executives in the public and private sectors.

Credits

Kieran Colvert
Hsiuwen Liu
Carey Vail
Editors
Ester Wensing
Art Director
Harry Harrison
Illustrator (cover)
Images
Getty Images

Contributors to this edition

Rupert Chamberlain
Alva Lee
KPMG China
Jenny WY Yu
Raymond NH Chan
Johnson Stokes & Master

Advertising sales enquiries

Ninehills Media Ltd
Tel: (852) 3796 3060
Jennifer Luk
Email: jennifer@ninehillsmedia.com

Ninehills Media Ltd

12/F, Infinitus Plaza
199 Des Voeux Road
Sheung Wan
Hong Kong
Tel: (852) 3796 3060
Fax: (852) 3020 7442
www.ninehillsmedia.com
Email: enquiries@ninehillsmedia.com

ISSN 1023-4128

ninehills media

Contents

Cover Stories

Cybersecurity oversight under Hong Kong's new critical infrastructure law 06

This article updates readers on Hong Kong's upcoming critical infrastructure legislation and the governance professional role in strengthening oversight, crisis planning and organisational resilience.

From penetration testing to red teaming 10

This article explores how governance leaders can transform cybersecurity from a compliance exercise into a driver of resilience and trust.

In Conversation

Tackling rolling bad apples 14

Alan Au, Executive Director (Banking Conduct), the Hong Kong Monetary Authority (HKMA), discusses the HKMA's Mandatory Reference Checking Scheme and how governance professionals can strengthen culture and conduct in financial institutions.

In Focus

Future-forward third-party risk management with managed services 18

This article explores how business leaders can tackle complex vendor risks efficiently.

Technical Update

Guidance note update 24

CGj provides a summary of the Institute's latest guidance notes published between April and September 2025.

Case Note

What directors should know about regulators' disciplinary trends 32

This article looks at the tightening regulatory focus on directors' accountability, due diligence and internal controls.

Giving Back

Edith Shih FCG(CS, CGP) HKFCG(CS, CGP)(PE) 36

Our new column, featuring members who volunteer their time to support the work of Council, launches this month with an interview with Edith Shih FCG(CS, CGP) HKFCG(CS, CGP)(PE), Honorary Adviser to Council, Past International President and Institute Past President, and Executive Director and Company Secretary, CK Hutchison Holdings Ltd.

施熙德女士 FCG(CS, CGP) HKFCG(CS, CGP)(PE) 38

我们的新专栏本月正式推出，专访支持公会运作的会员。首期嘉宾为公会理事会荣誉顾问、国际公会前会长及公会前会长、长江和记实业有限公司执行董事兼公司秘书施熙德女士 FCG(CS, CGP) HKFCG(CS, CGP)(PE)。

HKCGI News

President's Message 04

Institute News 40

Student News 46

Bulletin Board 48

Cybersecurity resilience

Managing cybersecurity risk has evolved into a vital governance concern in today's operating environment and this month's CGj takes a deep dive into this area of governance practice. Our cover stories look both at the rising regulatory expectations and at the most effective ways to boost organisational resilience in the face of an alarming expansion in cybersecurity threats.

First up, we assess an important milestone in our local cybersecurity regulatory regime. The Protection of Critical Infrastructures (Computer Systems) Ordinance (2025), due to become effective in January 2026, will make it a statutory obligation for organisations designated as critical infrastructure operators to have robust cybersecurity governance frameworks in place.

Our second cover story looks at two techniques – penetration testing and red teaming – designed to evaluate cyber resilience. The former tests specific IT assets for vulnerabilities, while the latter tests whether an organisation's overall cyber defences are effective by simulating real-world attacks on its systems and networks.

Both cover stories emphasise the pivotal role that members of our profession play in cybersecurity governance. In particular, two aspects of our work make us uniquely well positioned to bring value. Firstly, as an information hub and facilitator of cross-departmental collaboration, governance professionals can bring together various stakeholders – including senior managers, board members and IT professionals – to ensure that cybersecurity frameworks are effective and that they are aligned with the organisation's risk appetite and strategic objectives. The key message here is that cybersecurity cannot be siloed as solely an IT issue – it is an enterprise-wide concern and must be fully integrated into wider risk management and governance frameworks.

The second, and certainly no less important, aspect of the governance professional role in cybersecurity governance relates to our board support work. Another recurring theme in this month's cover stories is the crucial importance of effective board oversight. In this context, our role in strengthening the capacity of boards to understand and respond to the ever-expanding threat landscape has become a core part of our responsibility.

As usual, this month's journal includes a host of other useful articles and, before I conclude, I would like to add my commendations for the new Giving Back column launching in this month's CGj. This column will feature interviews with the unsung heroes of the Institute's work. Our Institute has been very successful in maximising the impact of our initiatives by drawing on the knowledge and expertise of a wide network of individuals both inside and outside our membership. Whether as members of our Council, of our committees, panels and working groups, or external collaborators who have joined forces with us in our research and advocacy initiatives, these individuals make an invaluable contribution to the profession.

Our first interviewee for this new column needs no introduction to readers of this journal. For three decades, Edith Shih FCG(CS, CGP) HKFCG(CS, CGP)(PE) has held top leadership positions in our Institute both locally and globally, and has become one of the Institute's best-known governance ambassadors. I am very happy to see our Institute and journal 'giving back' a small token of the credit and recognition she so rightly deserves.

David Simmonds FCG HKFCG

构筑网络安全的稳健基石

在当今运营环境中，有效管理网络安全风险已发展成为公司治理的核心议题。本月会刊将深入探讨这一重要治理实践领域。本期封面专题既聚焦日益提高的监管要求，也系统分析了在网络安全威胁持续升级的背景下，提升组织防御能力的有效路径。

首篇封面专题关注本地网络安全监管体系的重要里程碑——《关键基础设施（计算机系统）保护条例（2025年）》将于2026年1月正式生效。该条例明确规定，被认定为关键基础设施运营者的机构必须建立完善的网络安全治理框架，这已成为其法定义务。

第二篇封面专题重点解析了两种评估网络防御效能的专业方法——渗透测试与红队演练。前者针对特定信息技术资产进行漏洞检测，后者则通过模拟真实攻击场景，全面检验组织网络防御体系的整体有效性。

两篇封面专题共同凸显了治理专业人士在网络安全治理中发挥的关键作用。特别值得关注的是，我们在以下两个维度的独特价值：首先，作为信息枢纽与跨部门协作推动者，治理专业人士能够统筹管理层、董事会及信息技术部门等各方利益相关者，确保网络安全框架既具备防护实效，又与组织的风险承受能力及战略目标保持协同。核心要义在于：网络安全绝非单纯的技术议题，而是关乎全局的企业要务，必须全面融入整体风险管理与治理体系。

其次，治理专业人士在网络安全治理中的另一项关键职责，在于为董事会提供专业支持。本月封面专题中反复强调的另一核心议题，便是董事会有效监督职能的至关重要性。在此背景下，我们肩负的核心使命在于持续强化董事会对网络安全威胁态势的认知与应对能力——面对持续演变的网络威胁格局，这项职责已成为我们专业担当中不可或缺的部分。

延续会刊一贯特色，本期还收录了多篇实务佳作。特别值得关注的是，本月会刊新设的薪传治理专栏正式亮相。该专栏将聚焦那些在公会建设中默默奉献的幕后功臣。长期以来，公会通过整合会内会外的专业智慧与丰富经验，在提升各项倡议影响力方面取得显著成效。无论是担任公会理事会成员，各专业委员会、工作小组成员，还是作为研究及倡导计划的外部合作者，这些同仁均为行业进步作出了不可磨灭的贡献。

本月会刊新专栏首推的受访者对会刊读者而言早已耳熟能详。三十年来，施熙德律师 FCG(CS, CGP) HKFCG(CS, CGP)(PE) 在公会本地及国际层面持续担任领导要职，已成为公会最具影响力的治理倡导者之一。我谨藉本刊向她表达诚挚敬意，以此微薄礼赞，回馈她当之无愧的专业殊荣。

司马志先生 FCG HKFCG

Cybersecurity oversight under Hong Kong's new critical infrastructure law

Gabriela Kennedy, Partner, Mayer Brown Hong Kong LLP, and Pokit Lok, Principal of Risk Advisory Services, BDO Hong Kong, shared their thoughts with CGj on how Hong Kong's upcoming critical infrastructure legislation is challenging governance professionals to strengthen oversight, crisis planning and organisational resilience.

Hong Kong's Protection of Critical Infrastructures (Computer Systems) Ordinance (2025) marks a turning point in the city's approach to cybersecurity. Long treated as a matter of internal IT policy or voluntary compliance, cybersecurity will, for the first time, be subject to binding statutory obligations for organisations designated as critical infrastructure operators (CIOs).

The Ordinance, which was gazetted on 28 March 2025 and which will come into effect on 1 January 2026, responds to rising global concerns about cyberattacks targeting energy grids, transportation networks, telecommunications and other essential services. Through certain regulating authorities, the government is also expected to issue detailed codes of practice and guidelines in due course to assist CIOs with compliance.

The Ordinance defines two categories of critical infrastructure. The first covers infrastructures essential to the continuous provision of services in eight designated sectors – energy, IT, banking and financial services, air transport, land transport, maritime transport, healthcare services, and telecommunications and broadcasting. The second category, to be designated later by the government, includes other infrastructures whose damage, loss of functionality or data leakage could substantially disrupt Hong Kong's societal or economic activities.

From best practice to legal duty

For boards and governance professionals, the law signals a new era. Until now, many Hong Kong companies treated cybersecurity through voluntary frameworks or as part of enterprise risk management. Directors would receive periodic reports from IT teams, commission an audit after a breach and rely heavily on technical staff to assure resilience.

The Ordinance changes the dynamic, explained Gabriela Kennedy, Partner, Mayer Brown Hong Kong LLP. Once a company is designated as a CIO, it is required to maintain an office in Hong Kong, establish and maintain a dedicated computer-system security management unit, and appoint a qualified individual to oversee it. A CIO must also ensure the timely preparation and submission of a comprehensive computer-system security management plan, conduct annual cybersecurity risk assessments, arrange for computer-system security audits every two years, and/or as requested by the regulator, and develop and file detailed emergency response plans. In addition, the Ordinance imposes strict incident notification requirements, mandating that computer-system security incidents be reported to the Commissioner of Critical Infrastructure (Computer-system Security) within the prescribed period. Failure to comply exposes organisations to fines of up to HK$5 million and potential criminal liability for the entity.

'The Ordinance essentially elevates many cybersecurity measures that were previously regarded as best practice to mandatory obligations for designated CIOs,' said Ms Kennedy.

For boards, this means a fundamental shift in oversight responsibilities. 'While the Ordinance does not impose direct personal liability on directors or officers, the scale of potential penalties, the risk of operational disruption and the reputational consequences of enforcement actions significantly increase the board's obligations in relation to cybersecurity oversight,' Ms Kennedy warned.

Rethinking the board's role

Under the new Ordinance, boards can no longer treat cybersecurity purely as a technical matter. Cybersecurity must now be woven into governance structures, strategy and fiduciary duties.

Highlights

- the Ordinance will transform cybersecurity oversight from a discretionary practice into a statutory obligation for designated critical infrastructure operators
- boards must move beyond treating cybersecurity purely as a technical issue, to actively embedding it in governance structures, risk management frameworks and corporate culture
- governance professionals play a pivotal role in translating complex statutory requirements into actionable policies, bridging the gap between regulators, management and boards

> **the Ordinance essentially elevates many cybersecurity measures that were previously regarded as best practice to mandatory obligations for designated CIOs**
>
> **Gabriela Kennedy, Partner, Mayer Brown Hong Kong LLP**

Pokit Lok, Principal of Risk Advisory Services, BDO Hong Kong, recommends structural reforms at the board level. 'Boards should embed cybersecurity oversight in governance by establishing explicit accountability mechanisms, such as by forming a cybersecurity committee or appointing a chief information security officer with direct reporting lines. This aligns with the Ordinance's requirement for CIOs to designate responsible personnel and maintain robust cybersecurity governance.'

Mr Lok also emphasised the need for continuous monitoring of cyberthreats and integration of cybersecurity metrics into enterprise risk management. 'Boards should oversee the development of dashboards that track threat levels, response times and system vulnerabilities,' he suggested.

Ms Kennedy added that cyber risks should sit alongside other principal risks in board reporting. 'Boards should require management to regularly assess, monitor and report on cyber risks alongside other principal risks, and should also understand the company's most critical assets, the potential business impact of cyber incidents, and the effectiveness of controls in place,' she said.

For boards lacking technical expertise, Ms Kennedy stressed the importance of capacity building. 'Given the complexity and evolving nature of cyberthreats, boards should assess whether they possess sufficient collective knowledge to provide effective oversight. This may involve recruiting independent non-executive directors with direct experience in cybersecurity, information technology or risk management,' she said.

The Ordinance also introduces mandatory security drills, but both Ms Kennedy and Mr Lok believe boards should go further. 'Boards should require management to conduct periodic drills or tabletop exercises to test readiness, as well as to clarify roles and responsibilities in the event of a cyber incident. CIOs are required to submit and implement an emergency response plan and report a computer-system security incident to the Commissioner as soon as practicable – and in any event within the specified timeframe,' said Ms Kennedy.

Technical compliance, however, is only part of the puzzle. Ms Kennedy and Mr Lok agreed on the essential need for cultural change. 'Boards play a critical role in setting the tone from the top and fostering a culture of cybersecurity readiness throughout the company. This involves supporting ongoing employee training and awareness programmes, and ensuring that cybersecurity considerations are embedded in business decision-making at all levels,' Ms Kennedy explained.

Mr Lok echoed this view, citing the emphasis placed on computer-system security training and training programmes for all relevant personnel in the proposed outline for a code of practice included in the brief to the Legislative Council in relation to the Ordinance. 'Boards play a key role in fostering a cybersecurity-aware culture. This includes supporting training programs and awareness initiatives to ensure staff understand their responsibilities in protecting critical computer systems,' he said. 'By embedding cybersecurity in governance structures, boards not only meet legal obligations but also strengthen resilience, stakeholder trust and long-term value protection.'

'In short, the Ordinance raises the bar for board accountability in cybersecurity, making it a core governance responsibility with legal and reputational consequences,' Mr Lok said.

The role of governance professionals

Ultimately, directors cannot manage cybersecurity alone. Governance professionals will play a critical role in translating regulatory obligations into actionable practices. 'Governance professionals are responsible for developing, reviewing and updating cybersecurity policies and procedures, ensuring these are coherently communicated and consistently understood throughout

the organisation,' Ms Kennedy stated. 'They also foster a culture of cyber awareness and accountability by supporting staff training, encouraging prompt incident reporting, and embedding cybersecurity considerations into daily business operations and decision-making.'

Mr Lok elaborated on this theme, pointing out that governance professionals translate complex statutory obligations into clear internal policies, track compliance timelines and maintain audit trails, advise directors on emerging risks and oversee third-party providers to ensure adherence to security standards. In the event of an incident, they coordinate reporting and liaise with both the company's computer-system security management unit and the relevant authorities. This multifaceted role is essential to ensuring that boards are able to discharge their statutory duties while maintaining operational resilience.

Governance blind spots

Despite the Ordinance's detailed requirements, both Ms Kennedy and Mr Lok warned that boards could still overlook critical vulnerabilities. Ms Kennedy flagged up overreliance on internal controls. 'A common blind spot is the board's tendency to assume that implementing technical controls alone equates with genuine resilience, while overlooking the importance of governance processes that transform these controls into ongoing and sustainable organisational practice,' she said.

Ms Kennedy also strongly advised against ignoring third-party risks. 'Organisations should proactively manage vendors' risks by conducting regular assessments of vendor security practices, establishing specific incident reporting protocols, setting expectations through robust contracts and integrating third-party risks into the organisation's overall risk management framework. Tabletop exercises that involve third-party suppliers can be a good way to test responses in the event of a third-party breach,' she said.

Mr Lok identified additional operational blind spots, particularly in the area of operational technology. 'Boards often prioritise IT systems over operational technology, neglecting vulnerabilities in legacy industrial control systems such as programmable logic controllers. These systems, common in the energy, transport and utilities sectors, are often not designed with modern cybersecurity in mind, yet are integral to critical infrastructure operations,' he explained.

Mr Lok also called attention to the dangers inherent in any failure to appropriately escalate issues, cautioning that boards may lack predefined escalation criteria to distinguish between routine issues and reportable breaches, risking delayed reporting and non-compliance.

Strengthening crisis preparedness and backup resilience

Both Mr Lok and Ms Kennedy agreed that boards must approach crisis planning and backup services as a core governance responsibility. Mr Lok emphasised that this responsibility now has a dual dimension. 'Boards must ensure crisis planning and backup services align with both legal obligations under the Ordinance and their fiduciary duties to safeguard operational resilience and stakeholder interests,' he said. He highlighted the Ordinance's requirement for emergency response plans under Section 27 and stressed that these should be 'regularly reviewed and tested through drills and simulations'. Mr Lok also pointed out that backup systems and data recovery protocols should be secure, geographically diversified, and aligned with risk assessments and recovery objectives, with compliance closely monitored against the forthcoming codes of practice.

Ms Kennedy similarly affirmed the importance of going beyond paper compliance. 'Boards should require that crisis response and backup systems are properly documented and independently tested on a regular basis. This means going beyond internal reviews or checklists to include security audits and realistic simulations such as tabletop exercises and live security drills,' she said. Ms Kennedy explained that the results of such exercises should be reported directly to the board, with clear recommendations and action plans for addressing any identified weaknesses or gaps. She further urged boards to regularly review the adequacy of cyber insurance coverage to confirm it aligns with the organisation's risk profile and to ensure robust contractual terms with third-party providers, together with comprehensive communication protocols for transparent engagement during a crisis.

From penetration testing to red teaming

Why boards must rethink cybersecurity oversight

Kok Tin Gan, Partner, Cyber Security & Privacy, PwC, talks to CGj about how governance leaders can transform cybersecurity from a compliance exercise into a driver of resilience and trust.

Hong Kong is facing an unprecedented rise in cyberthreats. According to the Hong Kong Computer Emergency Response Team Coordination Centre, the number of cybersecurity cases in Hong Kong hit a five-year high in 2024 as hackers weaponised artificial intelligence (AI) to manipulate data systems and generate malware, impacting organisations across the public, private and non-profit sectors.

The consequences are increasingly tangible, from data loss and system outages to severe reputational damage. Against this backdrop, Kok Tin Gan shared his insights on how boards can move beyond tick-box compliance to build true organisational resilience.

Cybersecurity at the governance frontier

When directors discuss risk, cyberattacks now rank alongside financial, reputational and regulatory concerns. Mr Gan has worked with over 300 global security engagements and has coauthored cybersecurity guidelines for regulators. During that time, he has observed that as more people, products and services become connected, the need to proactively address cybersecurity and privacy risks has never been more urgent.

Mr Gan is the founder of the PwC's Dark Lab. This state-of-the-art technical space, based in Central, Hong Kong, is a dedicated space for simulating real-world hacking scenarios to help organisations identify vulnerabilities and prepare for sophisticated attacks. He explains that today's cyber landscape requires a forward-looking, hands-on approach, and that there are many ways to test an organisation's cyber resilience. Two of the most common are penetration testing and red teaming. However, many boards still struggle to distinguish between these approaches, which play very different roles in assessing and strengthening defences.

'Penetration testing is system-focused – it's about testing a defined application, like an e-commerce or email platform, for vulnerabilities. Red teaming is broader and is scenario-driven. This proactive approach looks at the pathways that an attacker could exploit if they wanted to breach your organisation. The goal isn't just to test systems, but also processes, people and response capabilities,' Mr Gan says.

He emphasises that both approaches have profound governance implications. Penetration testing is necessary but limited, only showing how individual systems might fail. Red teaming, on the other hand, provides directors with strategic insight.

'A red team exercise might reveal a forgotten VPN connection, or an HR platform accidentally left exposed to the internet,' Mr Gan notes. 'It tests whether detection and response mechanisms actually work, and whether management can react in real time. With red teaming, boards gain insight not only into technical weaknesses but also into cultural and organisational gaps.'

For governance leaders, cybersecurity should not be treated as a purely technical exercise. 'Security findings are not negative,' Mr Gan points out. 'They are essential for improvement. The philosophy is simple – find and fix. The more often you repeat that cycle, the stronger your organisation becomes.'

Asking the right questions

A recurring theme in Mr Gan's remarks is board engagement. He observes that too often, boards in Hong Kong are dominated by professionals without cyber expertise. 'I see many boards led by accountants and lawyers – these are valuable skills, but do not provide enough diversity

Highlights

- cybersecurity cases in Hong Kong reached a five-year high in 2024, driven by AI-powered attacks that targeted data systems and critical infrastructure across all sectors
- boards must move beyond tick-box compliance, using independent red team exercises and direct reporting to strengthen oversight and achieve meaningful remediation
- building the right board culture and expertise is essential, with diverse knowledge and transparency being essential for effective, long-term cyber resilience

> **“without the right people, boards don’t know how to interpret a red teaming report or how to challenge management effectively”**

of knowledge. Without the right people, boards don’t know how to interpret a red teaming report or how to challenge management effectively.’

Mr Gan argues that having the right people at board level is not simply about technical know-how, but about creating a culture where cyber issues are questioned with the same rigour as financial statements. He stresses that boards should move beyond treating policies as paperwork and instead ask questions that reveal whether processes, systems and people are genuinely secure.

What questions should directors ask? Mr Gan suggests starting with: ‘When was the last time we engaged an independent red team to test our environment?’ He advises boards to expect external qualified assessors to carry out exercises without informing management in advance, with findings reported directly to the board, along with all relevant remediation roadmaps.

He also encourages directors to tailor their questions to the organisation’s activities and markets. For instance, if a company is entering a new jurisdiction, boards should ask about local data protection laws and the cyber environment. If a company is moving operations to the cloud, they should probe vendor security standards and contractual safeguards.

Key indicators to monitor include:

- whether the scope of the assessment is impartial and comprehensive
- how management prioritises and remediates findings within set timelines, and
- whether systemic root causes, such as outdated patching processes or inadequate staffing, are addressed – it should not be just about the technical symptoms.

Preparing for emerging threats

Mr Gan highlights that due to the rapid advancement of technology, the threat landscape is expanding faster than most boards realise. Traditional entry points such as phishing, VPN exploitation and unpatched systems remain prevalent, but new risks are emerging.

‘Generative AI makes it easy to craft convincing phishing emails, videos or even voice messages. Attack surfaces are expanding across messaging apps, social platforms and blockchain systems. We are also seeing AI poisoning, where malicious actors manipulate training data to bias outcomes,’ Mr Gan warns.

For governance professionals, Mr Gan emphasises that cyber risks must be fully integrated into enterprise-wide risk management frameworks, not just treated as a siloed IT issue. Incident response playbooks should be designed with AI-powered and cross-border attacks in mind, recognising that attribution and enforcement are often slow and complex. Boards should also require regular, independent red team exercises, ensure that findings are reported directly to the board and track management’s remediation against clear timelines.

Beyond playbooks and reports, directors should promote a culture where security findings are seen as opportunities for improvement rather than failures, insist on diverse expertise within the board and ensure that budgets are tied to addressing root causes – such as patch management, third-party oversight and staff training – rather than focusing only on technical quick fixes.

Culture, DNA and the tone at the top

Mr Gan repeatedly returns to the importance of leadership tone. ‘Everyone says the tone at the top matters, but the real question is how to achieve the right tone. That comes from board composition, diversity of knowledge and a willingness to see cyber findings not as bad news, but rather as an opportunity to strengthen resilience.’

The DNA of governance – whether an organisation values transparency, continuous improvement or technical competence – ultimately determines whether cybersecurity is treated as a strategic imperative or as a compliance tick box.

> “don’t hide your bugs – find them and fix them”

Forward-thinking companies treat red teaming as a continuous process, rather than as a one-off audit. Tech leaders like Apple have institutionalised bug bounties that reward the discovery of flaws, reinforcing a culture of openness. Closer to home, regulators such as the Hong Kong Monetary Authority and the Securities and Futures Commission are issuing frameworks that expect boards to integrate cyber risk oversight into their fiduciary responsibilities.

For smaller organisations and NGOs with limited resources, Mr Gan’s advice is pragmatic, accepting that cybersecurity expertise is scarce and costly, but that it starts with culture. Even without a large budget, boards can embed ‘find and fix’ principles, periodically seek independent assessments and ensure cyber risks are integrated into strategic decision-making.

As digital dependency deepens, the role of boards in cybersecurity governance is no longer optional. Red teaming and penetration testing are not just technical tools, but are vital governance mechanisms that reveal blind spots, test resilience and sharpen oversight.

‘Don’t hide your bugs – find them and fix them,’ Mr Gan concludes. ‘The more you do this, the more secure your organisation becomes. That mindset is the foundation of effective cybersecurity governance.’

Tackling rolling bad apples

Phase 2 of HKMA's Mandatory Reference Checking Scheme

In July 2025, the Hong Kong Monetary Authority (HKMA) announced Phase 2 of the Mandatory Reference Checking (MRC) Scheme, which was implemented on 30 September 2025. Alan Au, Executive Director (Banking Conduct), HKMA, explains the policy thinking, overseas touchpoints, lessons from Phase 1 and how governance professionals can strengthen culture and conduct across financial institutions.

What motivated the HKMA to develop the MRC Scheme in the first place?

'The origins of the scheme trace back to the 2008 Global Financial Crisis. In the wake of that crisis, international reforms initially focused on strengthening the resilience of financial institutions, with measures targeting capital, liquidity, resolution regimes and market transparency. However, it soon became clear that an equally critical area, that of conduct and culture, was being overlooked.

In 2017, the HKMA launched its Bank Culture Reform to address this gap. The initiative was built on three interconnected pillars. The first pillar, governance, emphasises the importance of setting the right tone from the top, with strong board-level oversight to drive ethical behaviour. The second focuses on incentive systems, covering how institutions recruit, train, promote and reward staff, ensuring that the right behaviours are recognised and reinforced. The third pillar, assessment and feedback mechanisms, involves establishing effective monitoring tools such as dashboards and whistleblowing mechanisms, allowing senior management to hear and act on what I call the "echo from the bottom".

Despite these reforms, we cannot simply assume that bank staff will always act with integrity. From time to time, there are still some "bad apples" who engage in misconduct. When such actions are discovered, these bank staff, who damage the interests of customers for their own benefit, will often try to move on to another banking institution to evade the consequences and to repeat their misconduct, meaning that the risk of misconduct simply spreads – or "rolls" – from one firm to another. The MRC Scheme was developed specifically to close this gap by introducing a system-wide approach to identifying and addressing these risks.'

Why weren't traditional reference checks enough to catch misconduct risks?

'In the past, hiring traditionally relied on two tools – self-declarations by applicants and references from former employers. Both had limits. Individuals could simply choose not to disclose past investigations or internal disciplinary actions. Former employers generally restricted references to bare facts, such as dates and titles, but often felt unable to provide conduct-related information, such as details of any previous investigation or disciplinary action taken, due to potential litigation risks, or simply because records had just not been maintained in a way that supported meaningful disclosure.'

How has the MRC Scheme closed that gap?

'The scheme has introduced an industry-wide, mandatory protocol to ensure transparency and accountability in hiring. Candidates must first consent to reference checks, after which their previous employers are required to provide fact-based conduct information covering the past seven years using a standard template. The conduct information to be reported includes past disciplinary actions, incidents that cast doubt on an individual's honesty or integrity and any relevant ongoing investigations. To ensure fairness, any negative information triggers an opportunity to be heard. The candidate can explain or respond to the negative information before the hiring decision.'

What have you observed since Phase 1 went live?

'Phase 1 of the scheme was launched in May 2023, covering approximately 3,500 senior banking staff. These included senior executives such as the chief executive, alternate chief executives, directors and managers as defined under the Banking Ordinance, as well as executive officers and officers responsible for securities, insurance and Mandatory Provident Fund (MPF) business within banks.

Since the launch of the Phase 1, approximately 700 reference checks

Highlights

- the HKMA's MRC Scheme was developed to prevent individuals from moving between banks without disclosing their misconduct history
- Phase 2 expands the scheme's coverage to 50,000 banking practitioners, significantly broadening its reach across the sector
- the scheme complements wider cultural reforms aimed at fostering fair treatment of customers and long-term positive customer outcomes

> **“the scheme has introduced an industry-wide, mandatory protocol to ensure transparency and accountability in hiring”**

have been conducted under the scheme, with nine cases – about 1% – containing negative information. While the percentage is small, it is certainly meaningful, demonstrating that the scheme is able to uncover risks that would otherwise go undetected.

Looking ahead, this percentage may decline – not because the scheme is ineffective, but because individuals with a history of misconduct will recognise that they cannot bypass the scheme and will be deterred from seeking a position within the sector. This is precisely the scheme's objective, to prevent bad apples from rolling through the banking industry and causing further harm.'

What has changed in Phase 2?

'The scope of checks has been greatly expanded. Phase 2 will extend coverage to about 50,000 staff – more than half the banking workforce – including those licensed or registered to carry out securities, insurance or MPF regulated activities within banks. The same parameters apply, namely candidate consent, conduct-related reference information covering the past seven years using a standard template, and the opportunity to be heard. We have strong industry support for the expansion.'

Do you think the market's response to the MRC Scheme reflects a growing awareness of the importance of culture and conduct?

'Absolutely. There is definitely a much greater awareness now. Over the past few years, we have introduced a series of measures to strengthen culture and conduct across the banking sector. It is not something that can be addressed by a single initiative, which is why I emphasised earlier the broader framework we have built around the three pillars of sound bank culture – governance, incentive systems, and assessment and feedback mechanisms.

The MRC Scheme is just one part of the equation, expressly designed to tackle the issue of rolling bad apples. The scheme cannot transform culture on its own, but combined with other measures, it plays an important role in safeguarding the system and raising standards across the sector.

Our overarching goal is to achieve two key outcomes. The first is to ensure that firms and their staff treat customers fairly. This means selling suitable products, offering services that meet customers' needs and promoting financial inclusion. The second goal is to deliver good customer outcomes. When customers purchase a product today, they won't necessarily know whether it will still meet their needs three or five years down the line. It is therefore vital that frontline staff focus on identifying products that align with customers' long-term financial objectives and personal circumstances, rather than simply pushing a particular product to earn a higher commission or a bonus.'

Where can governance professionals add the most value?

'The first is the tone from the top. Senior leadership must clearly articulate the values and objectives they want to see embedded in the organisation. Banks, especially large retail banks in Hong Kong, are highly structured organisations with thousands of employees spread across multiple layers, from the board and top management to middle management, branch management and finally the frontline staff. The challenge lies in ensuring that the messages from the top are not confined to the boardroom, but instead filter through every level of the organisation.

The second element is the echo from the bottom. Leaders need to understand what is truly happening on the ground. You have to ensure that the messages, when they are filtered through, get internalised by your staff. They have to believe in the importance of treating customers fairly and of achieving good customer outcomes.

Of course, there are also practical tools that support this process. The MRC Scheme is one such tool. Plus, we are in discussions with other financial regulators about extending similar mechanisms beyond banking and into non-bank financial sectors, because misconduct does not stop at sector boundaries.' CGj

CHARTERED GOVERNANCE
Hong Kong

SAP

HKCGI Student Ambassadors Programme (SAP)

Begin your leadership journey in corporate governance!

Undergraduates & full-time master's students are welcome!

Registration fee: HKD120

CONNECT and SHARE:

☑ Mentorship Programme

☑ Unique Exposure:

- Visits to regulators and corporations
- Attend AGMs of listed companies

☑ Internships and Career Opportunities

☑ Networking Activities

- Meet governance professionals and fellow Student Ambassadors

☑ Professional and Soft Skills Workshops

Register Now!

(852) 2830 6039 student@hkcgi.org.hk www.hkcgi.org.hk

The Hong Kong Chartered Governance Institute 香港公司治理公會 (Incorporated in Hong Kong with limited liability by guarantee)

Future-forward third-party risk management with managed services

In this article, Rupert Chamberlain, Partner, Head of Managed Services, and Alva Lee, Partner, Head of Governance, Hong Kong SAR, KPMG China, explore how business leaders can tackle complex vendor risk landscapes efficiently.

Many organisations have become highly dependent upon external vendors for managing cloud and data, delivering business functions like finance and human resources, and handling logistics and warehousing. These vendors may in turn outsource to fourth parties. Without appropriate procedures in place, this leaves organisations vulnerable to cyberattacks and supply chain disruption, questionable labour and environmental practices, and poor-quality products and services that impact internal and external customers.

A large private or public entity must manage the risks associated with an army of third, fourth and fifth (or 'nth') parties that may run into the tens of thousands. The proliferation of fourth and fifth parties ('vendors of your vendors') – many of whom may have no direct contact with the organisation – takes risk management and operational resilience to a new level of complexity. The web of parties is greater than enterprises may realise, enlarging the attack surface with threats beyond the organisational line of vision.

As communications and transactions go digital, and significant numbers of people work remotely, the risk only rises. Third-party risk management (TPRM) encompasses a wide range of activities, from initial procurement and onboarding, ongoing management and monitoring, skilfully managing risk and driving improved performance through the lifecycle of the relationship. However, without clear and consistent accountability for TPRM, the risk of a damaging incident, or non-compliance, remains high.

In this article we discuss how Chief Technology Officers, Chief Information Security Officers, Chief Compliance Officers and Chief Procurement Officers can transform TPRM through managed services to reduce costs and increase efficiency, speed, scalability and operational resilience, as well as to preserve business continuity.

Today's big TPRM challenges

There is increasing pressure and regulatory scrutiny to meet demanding requirements for know your customer (KYC) and know your supplier (KYS) onboarding and monitoring, to verify that third parties are genuine, competent and financially viable, with sustainable business practices. These regulatory requirements include the:

- European Union General Data Protection Regulation
- European Union's Digital Operational Resilience Act, setting expectations of digital operational resilience for financial entities
- Hong Kong Monetary Authority guidelines for outsourcing and third-party arrangements, to ensure adequate governance and sound risk management controls, and
- Monetary Authority of Singapore's guidelines for outsourcing and third-party arrangements, to ensure adequate governance and sound risk management controls.

Risks can vary across sectors. For example, automotive manufacturers are highly focused on quality across their extensive, complex supply chains to ensure that vehicles are

Highlights

- the increasing reliance on vendors and more complex supply chains are heightening the risk of cyberattacks, compliance failures and supply chain disruptions
- managed services offer scalable, tech-driven solutions that centralise monitoring, reduce costs and speed up vendor onboarding
- a unified approach to third- and fourth-party risk enables organisations to build resilience and safeguard business continuity

> **without clear and consistent accountability for third-party risk management, the risk of a damaging incident, or non-compliance, remains high**

safe and perform consistently. The life sciences are heavily regulated, with companies having to verify the quality and safety of all ingredients and to show that outsourced activities – notably laboratory testing – are carried out to required standards. Industries like energy and telecommunications, which are vital to national security, need to demonstrate operational resilience along the entire value chain. Sectors with large customer databases, such as consumer and retail, and consumer financial services are obliged to meet strict data privacy and security demands and, increasingly, keep data within specific geographical boundaries. Meanwhile, nearly all organisations must comply with regulations on environmental, social and governance (ESG), data protection, anti–money laundering and sanctions.

Responsibility for TPRM varies, with functions like procurement, legal, compliance, risk management, data privacy, security and IT often dealing with different vendors. Tasks include carrying out due diligence, onboarding vendors, monitoring, performing onsite audits, developing incident reports, conducting certification searches and other activities. Procurement, in particular, has played a leading role in improving efficiency and the speed of delivery, while retaining strong risk management that matches the organisation's risk tolerance. These departments may well have their own data systems, as well as varying attitudes and appetite for risk, which could mean that some third parties receive less rigorous attention than others, increasing the chance of incidents, inadequate performance or non-compliance. Procurement's role in making high-quality buying decisions is often underutilised, presenting an opportunity for better vendor risk management. Many organisations are unable to gain a complete overview of all the risks associated with each third party, which can threaten organisational resilience.

On top of this, a fragmented approach to third-party risks – all too common amongst organisations today and frequently involving manual tasks – slows down decision-making, delays vendor onboarding and holds up operations.

Often missing is a holistic view on third-party risk across the entire ecosystem of vendors, as well as a consistent approach to managing these risks. There is a tendency for the various internal functions overseeing third parties to view risk purely in terms of KYC and onboarding. They may require additional perspectives to carry out appropriately thorough risk assessments and, as a result, could neglect the ongoing management and monitoring that is essential to stay on top of potential and evolving risks.

The case for managed services in TPRM

Outsourcing TPRM, as part of supply chain strategy, can bring significant benefits, offering a tailored service that integrates with existing IT infrastructure and processes, and which collaborates closely with the legal, compliance and procurement functions. Managed services providers take a 360-degree view of the risks facing third parties, helping to identify where threats may lie and to evaluate the impact of events. Risk assessment and monitoring become more centralised, enabling a standardised, comprehensive risk management approach that quantifies risks and reduces the chance of gaps or blind spots.

Here's how outsourcing TPRM through managed services can help address critical pain points like speed, monitoring, scalability and cost-efficiency, while leveraging cutting-edge technologies to streamline risk management.

Speed

A huge priority for TPRM – as delays in onboarding can clog up vital supply sources, while any delay in identifying

problems can have a severe impact on costs, compliance and reputation.

Monitoring
Through continuous monitoring of systems and networks, potential issues are identified before they escalate, maintaining business continuity by reducing downtime and interruptions.

Collaboration
By fostering collaboration and clear communications between internal teams and external vendors, providers minimise misunderstandings and align interests.

Scalability
Providers are also likely to gain sufficient scale (and the capability to scale up or down quickly if necessary) to handle the massive volumes of third- and fourth-party vendors that large organisations typically interact with. Such flexibility not only helps manage seasonal demands and rapid growth, but does so without compromising service quality.

Cost
Many managed services providers operate on a subscription model, making costs more predictable and eliminating the need for large, upfront capital expenditure.

Resources
For overstretched risk management teams, a managed services team provides additional resources to fill in expertise and capability gaps, and bring in the latest technologies – something that may be unaffordable for many organisations. Through careful prioritisation of risk management, based upon the expected risk levels of different vendors, resources can be further optimised to focus on those parties where potential risks are highest. An experienced managed services provider has addressed crises in the past and should have a fast, proven streamlined and methodical recovery methodology, to speed up the return to business-as-usual.

Technology
Leading managed services companies invest heavily in the latest technology. Artificial intelligence (AI), automation and machine learning achieve real-time – or near-real-time – monitoring, which could, for instance, trace a failure of suppliers to maintain appropriate environmental standards. Additionally, intrusion detection systems and encryption protect sensitive data and help achieve compliance with security standards. Generative AI has exciting potential to ease the management of vendors, gather large amounts of data from disparate systems, translate documents into common languages and produce insightful reports.

By integrating cloud-based, portal-driven solutions, along with predictive analytics for proactive risk management, organisations can increase their understanding of vendors along the supply chain and spot problems early – or even in advance – enabling swift action to prevent disruptions and improve resilience. This might, for example, help identify a supplier in financial difficulties before its condition becomes critical. These insights also enable informed decisions on vendor relationships and risk management strategies.

With large-scale automation replacing manual processes, and integrated systems and processes reducing waste and duplication, TPRM costs should decrease. This is a great example of accessing technology through partners to improve the quality of management information and to assist decision-making – such as whether or not to retain suppliers – as well as to gain cost efficiencies.

Regulations
Critically, as third- and fourth-party risk specialists, a global managed services provider keeps abreast of the latest international, national and regional regulatory requirements. Such knowledge, allied with strong governance, helps ensure that third parties meet evolving requirements, including cybersecurity, data privacy and ESG performance across the supply chain – reducing the chance of penalties and/or reputational damage. Although there have been pushbacks in some countries, the requirement for comprehensive ESG assessments of third parties is growing.

Four key features of an efficient managed services model

Pre-contract due diligence
Pre-contract due diligence is a risk-based approach to vendor assessments to identify any potential problems early. Streamlined compliance with privacy and cybersecurity mandates should speed up the onboarding process so that

it considers the third party's true capabilities, going beyond a mere 'tick-the-box' exercise. Important new suppliers and contractors can get to work faster, bringing value to the organisation and enhancing the vendor experience to get the relationship off to a good start.

Ongoing monitoring and incident handling

Ongoing monitoring and incident handling involves continuously evaluating vendor performance against service level agreements to preserve high standards and act when performance levels fall below what is required. Methodologies such as ITIL (previously known as Information Technology Infrastructure Library) or Six Sigma drive improved efficiency and performance. AI and other technologies are rapidly transforming the landscape, and can be used to enhance monitoring and to detect any breaches or deviations faster and more comprehensively. For example, by leveraging an AI-powered tool to efficiently and consistently analyse vendor SOC (system and organisational controls) 1 and SOC 2 reports, organisations can benefit from analytics and insights for more risk-intelligent decision-making. The results of incident handling should trigger further monitoring or adjustments to the risk classification of the third party.

Robust governance frameworks

When provided by managed services providers via clear roles, responsibilities and escalation protocols, robust governance frameworks can be applied consistently across the organisation. Regular audits and performance reviews not only assess vendor quality but can also uncover weaknesses or inefficiencies that could lead to problems in the future.

Fourth-party risk management

Fourth-party risk management uses software and research to trace risks across extended supplier networks.

TPRM is evolving to encompass far more than just compliance

When leveraged effectively, TPRM can be a significant strategic enabler that helps organisations optimise their supply chain strategy beyond the direct outcomes, swiftly onboard vendors and optimise the value they bring, as well as reduce the risk of penalties, supply chain disruptions and reputational damage.

To evaluate the opportunity in your TPRM programme, consider these questions:

- Do you have a holistic view of third-party risk across all vendors?
- Do you have unified data systems across procurement, legal, compliance and other business functions?
- Can you quickly identify and address suppliers at risk?
- Can you keep up with fast-changing regulatory compliance requirements?
- Are you able to quickly and confidently onboard new suppliers?

> **"managed services providers take a 360-degree view of the risks facing third parties, helping to identify where threats may lie and to evaluate the impact of events"**

If the answer is 'no' or 'uncertain' to any of these questions, then it may be time to make a change. For many companies, managed services are a compelling solution.

This operating model – enabled by AI and other technologies, as well as a suitably skilled and savvy team – can accelerate the transformation of TPRM to become more proactive, avoid risks and incidents, and extract better performance from your extended ecosystem. A multistakeholder approach, with a single data repository, involving legal, compliance and procurement teams in risk management discussions, and augmented by a managed services provider, can drive innovative new ways to manage third- and fourth-party risk, and to build trust.

Rupert Chamberlain, Partner, Head of Managed Services, and Alva Lee, Partner, Head of Governance, Hong Kong SAR
KPMG China

CHARTERED GOVERNANCE
Hong Kong

HKCGI

ECPD Videos on Demand

Board Effectiveness Series:

- HK Listing Rules New Board Effectiveness Evaluation Requirements - Sharing on International Best Practice
- Future-Proofing Governance: From Paper to Platforms as a Key to Board Effectiveness
- Onboarding - A Practical Guide for Directors

Wealth Management Series

- New Company Re-Domiciliation Regime and Latest Trends in Tax Controversy
- Hong Kong Payroll Management: Practical Brief and Update
- Overview of Taxation for Doing Business in China

Anytime anywhere at your convenience

Register *now!*

For more details, please check the Professional Development section of HKCGI website: www.hkcgi.org.hk

Enquiries: 2830 6011 / 2881 6177 / cpd@hkcgi.org.hk

Guidance note update

CGj provides a summary of the Institute's latest guidance notes published between April and September 2025, covering a wide range of topics from greenwashing and whistleblowing to NGO governance and the new stablecoin regulatory regime.

As an integral aspect of its thought leadership and professional development initiatives, the Institute routinely publishes guidance notes to keep governance professionals and practitioners in Hong Kong and the Chinese mainland abreast of the latest developments in governance, risk and compliance.

Apart from the four themes featured in this article – greenwashing, whistleblowing, NGO governance and Hong Kong's new stablecoin regulatory regime – the Institute's guidance notes issued in the second and third quarters of 2025 covered a number of pertinent topics, comprising A-then-H listings, preparing for the USM regime, the upcoming critical infrastructure bill, virtual asset staking, the new company redomiciliation regime, digitalisation and competition law, digital investigations and compliance priorities for directors.

Greenwashing

This two-part guidance note, titled Greenwashing: A Corporate Strategy for Sustainability Credibility, provides a practical overview of what greenwashing is, how it can undermine ESG and sustainability credibility, and what governance professionals can do to mitigate the risks.

Part one defines greenwashing as a form of corporate misrepresentation, 'whereby companies make misleading or unsubstantiated claims about the environmental benefits or sustainability of their products and services, or unrealistic or unverifiable assertions regarding their decarbonisation efforts and net-zero goals'. It identifies several types of greenwashing, including overly generalised terms and irrelevant claims, cautioning that such practices can erode stakeholder trust and attract regulatory scrutiny, which can impact brand perception and, ultimately, financial performance.

The guidance warns that beyond reputational damage, the legal and financial consequences are escalating globally. For example, in the EU, the UK, the US, Canada, Australia and Singapore, anti-greenwashing regulations now impose stricter requirements on environmental claims, with guardrails around language use and the evidentiary standards that corporates must meet.

In Hong Kong, while there is still no specific greenwashing-related legislation, regulatory expectations are rising in parallel with international developments. The guidance note observes that the Securities and Futures Commission and the Stock Exchange of Hong Kong are both becoming increasingly vigilant regarding ESG and sustainability reporting accuracies for listed companies. 'Hong Kong will need to focus on tackling greenwashing as part of its ambition to be a leading international sustainable financial centre,' the guidance note advises.

It also stresses the importance of a strong governance framework, noting that 'governance professionals must raise awareness of the issue, steer their organisation away from greenwashing practices, and facilitate training for directors, other executives and frontline staff,' especially in the ESG reporting process.

Highlights

- regulatory and stakeholder expectations in relation to greenwashing in Hong Kong are rising in parallel with international developments
- governance professionals play a key role in implementing whistleblowing frameworks, including developing clear policies on reportable matters and establishing protections against retaliation
- governance professionals can provide NGOs with a comprehensive roadmap for strengthening board effectiveness, financial oversight and risk management, while fostering a culture of integrity to support sustainable mission impact

Part two of the guidance note pinpoints various measures companies can take to manage and mitigate greenwashing-related risks, particularly for those with a consumer-facing business or an international presence.

The first step is to understand the company's regulatory obligations. This begins with mapping out all jurisdictions where the company operates or markets its products to identify relevant greenwashing-related laws and regulations. Even in markets without explicit greenwashing rules, 'companies should understand how existing consumer protection, securities and advertising laws might apply to sustainability claims', the guidance note recommends.

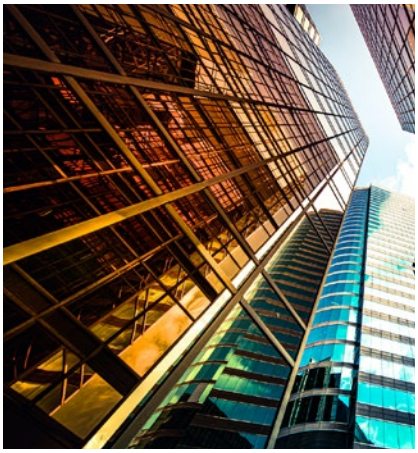
The second step is to benchmark against global best practices. Beyond complying with current regulations, companies should monitor emerging global greenwashing regulations to stay ahead of future legal developments and stakeholder expectations. This helps determine whether meeting baseline regulatory requirements is sufficient or whether higher standards are needed to manage reputational risks.

The guidance note offers five key takeaways that governance professionals should consider advising their companies to embed within their governance frameworks.

1. understand the company's risk profile

2. ensure operational alignment

> **"Hong Kong will need to focus on tackling greenwashing as part of its ambition to be a leading international sustainable financial centre"**



3. establish a robust ESG data infrastructure

4. select appropriate ESG metrics, and

5. commit to being transparent.

'Greenwashing risk management should not be viewed merely as compliance-driven risk mitigation, but rather as an opportunity to enhance reputation by building lasting consumer trust through transparency and integrity in sustainability communications,' it concludes.

Whistleblowing

Part one of the Institute's Ethics, Bribery and Corruption Interest Group guidance note on whistleblowing, titled Whistleblowing – The Software and the Hardware to Thrive, published in January 2024, introduced the concept and explained how governance professionals can help their organisations develop a culture that encourages whistleblowing and ethical conduct. Part two, published in April 2025, sharpens attention on the operational elements needed by listed companies to make whistleblowing schemes credible and effective.

Under the Corporate Governance Code Provision D2.6, listed companies must establish a whistleblowing system that allows employees and external stakeholders to report concerns confidentially and anonymously to the audit committee or a majority-INED committee, on a 'comply or explain' basis. Code Provision D3.7 further requires the audit committee to ensure proper arrangements for confidential reporting, independent investigation and follow-up. Whistleblowing is positioned as part of the company's risk management framework, with oversight from the board and with operational responsibility resting with the audit committee and the governance professionals supporting policy implementation and review.

Recent ESG governance reforms have also upgraded expectations around board-level oversight. 'A credible whistleblowing system – especially one that captures concerns raised by employees and external parties

> **a credible whistleblowing system – especially one that captures concerns raised by employees and external parties – is a foundational component of a company's ethical infrastructure**

– is a foundational component of a company's ethical infrastructure. It is also a signal to investors that the company takes integrity seriously,' the guidance note explains.

Governance professionals play a vital role in implementing whistleblowing frameworks. This includes developing clear policies that define reportable matters, outlining confidential reporting procedures and establishing protections against retaliation, with oversight typically assigned to the audit committee. Accessible reporting channels, such as email, hotlines or third-party platforms, are also essential to encourage reporting from both staff and external stakeholders.

Ongoing training and communication, incorporating the Independent Commission Against Corruption's Anti-Corruption Programme, A Guide for Listed Companies, helps normalise whistleblowing as a constructive tool and reinforces the organisation's commitment to integrity. Governance teams must also maintain robust internal processes for logging, investigating and escalating complaints, preparing reports for the audit committee and conducting regular policy reviews with internal audit and board oversight to ensure continued effectiveness and credibility.

The guidance note also points out that, despite clear requirements under the Listing Rules, whistleblowing systems often face challenges such as box-ticking disclosures with little evidence of effectiveness, limited capacity within audit committees to manage whistleblowing risks and the absence of dedicated legal protections for whistleblowers in Hong Kong. This places greater responsibility on companies to build trust through strong internal safeguards. Additionally, weak or opaque whistleblowing practices can harm international perceptions of a company's governance maturity, even if no regulatory breach occurs.

NGO governance

The latest guidance note issued by the Institute's Public Governance Interest Group, titled NGOs and Governance Professionals' Contributions, is a four-part publication designed to help governance professionals ensure accountability, integrity and sustainability in non-governmental organisations (NGOs), without overburdening these often resource-constrained entities.

Part one of the guidance note highlights how governance professionals can play a pivotal role in strengthening NGO governance, particularly around board composition and independence. Many NGOs, especially founder-led or community-based ones, struggle with boards made up of close associates, which may lack the objectivity and diversity of expertise needed for effective oversight. 'A well-structured board is the cornerstone of good governance in any NGO,' the guidance note asserts.

Governance professionals can assist in a number of ways, including by encouraging board rotation and renewal, guiding independent and

> **“a well-structured board is the cornerstone of good governance in any NGO”**

skills-based recruitment, defining and clarifying the distinct roles and responsibilities of the board and senior management, and helping manage founder succession and the transition toward more sustainable governance structures. In addition, as clarity of purpose is paramount for NGOs to remain effective and accountable, governance professionals can help by facilitating strategic planning, reviewing funding proposals, developing reporting frameworks, and supporting both internal and external communications.

Part two looks at how governance professionals can strengthen transparency and financial oversight, as well as ensure an NGO complies with all legal and regulatory obligations. ‘The governance professional helps protect the NGO’s financial integrity by implementing strong financial oversight and transparency practices. This ensures that funds are used efficiently and for their intended purpose, and bolsters the NGO’s reputation among donors, regulators and the public, leading to continued support and growth,’ the guidance note states. Furthermore, the governance professional can guide the NGO in identifying potential legal and regulatory risks, and offer proactive measures to manage and mitigate such risks.

In part three, the guidance note turns to operational governance, in particular how governance professionals can enhance NGO effectiveness by helping to establish and manage board committees tailored to specific organisational needs. Such committees could comprise core audit and finance, nomination and remuneration committees, as well as additional committees such as fundraising, risk management, HR, programmes, and marketing and communications committees, depending on the particular needs of the NGO. For smaller NGOs with limited resources, the governance professional could recommend the formation of an overall governance committee to coordinate several functions. By guiding committee formation and clarifying roles, governance professionals can help NGOs professionalise operations while preserving the integrity of their mission.

The fourth and final part of this guidance note explores the role that governance professionals can play in helping NGOs navigate the complexities of governance, risk and strategy, and in sustaining and amplifying the mission-driven work of NGOs, beyond merely establishing relevant governance structures. The guidance provides a clear framework for governance professionals to build a culture of integrity and ethical behaviour, to develop board capacity and effectiveness, and to enhance risk management, internal controls and strategic planning.

Stablecoin regime

This three-part guidance note, titled Governance Considerations under Hong Kong’s New Regulatory Regime for Stablecoins, provides governance professionals with a clear roadmap to navigate the city’s new licensing regime for stablecoin issuers.

Part one sets the foundation by explaining the Stablecoins Ordinance, which came into effect on 1 August 2025. Under this framework, the issuance of fiat-referenced tokens will be subject to licensing, while algorithmic stablecoins are expressly prohibited. The guidance clarifies key definitions, including specified stablecoins, which are fiat-backed tokens designed to maintain a stable value relative to an official currency, and active marketing, which refers to any promotional or solicitation activity directed at the Hong Kong public that could reasonably lead to the use or adoption of a stablecoin. It also outlines the activities that fall within the regulatory parameters – issuance, offering, marketing and related operations – all of which will require authorisation.

Part two explores the licensing criteria and supervisory expectations that stablecoin issuers will need to meet. A core principle is the full backing of outstanding specified stablecoins by high-quality, liquid reserve assets held in the same referenced currency, with reserves segregated from other company assets and safeguarded from creditor claims. Beyond financial soundness, the guidance note sets out expectations around internal controls, risk management and independent

audit. Governance professionals are called on to advise boards on policies governing issuance, redemption and distribution, ensuring that these are carried out in a prudent, transparent and compliant manner. The guidance note also highlights governance structures, noting the requirement for key personnel to be 'fit and proper' and for boards to include a significant proportion of independent directors. Collectively, these measures point to a regime that demands high standards of governance and accountability, with governance professionals central to guiding entities through the complexity.

Part three turns to enforcement and transition. The Hong Kong Monetary Authority is empowered to issue reprimands, financial penalties or even licence bans, with appeals channelled through a dedicated tribunal. Licensed stablecoin issuers will also fall within the ambit of Hong Kong's anti–money laundering and counter–terrorist financing regime, requiring enhanced due diligence, transaction monitoring and ongoing compliance. Transitional arrangements provide a six-month grace period for pre-existing issuers that apply for licences within the first three months of the regime. The guidance note closes with a governance readiness checklist, encouraging entities to assess their board oversight, risk controls, technology resilience and disclosure protocols.

> *The guidance notes covered in this article are available in the Thought Leadership section of the Institute's website: www.hkcgi.org.hk.*

Guidance note roundup

The HKCGI guidance notes published in the second and third quarters of 2025 are set out below. The Institute would like to thank everyone involved in their production.

April

Guideline for A-then-H Listings. This Chinese-language HKCGI guidance note, outlining key execution strategies for A-then-H listings and post-listing compliance requirements for dual A+H share listings, was published in collaboration with Baker McKenzie FenXun.

Greenwashing: A Corporate Strategy for Sustainability Credibility (Parts 1 and 2). This two-part HKCGI guidance note was authored by Ben McQuhae, Founder, Jessica Ha, Associate, and Angela Cheng, Consultant, Ben McQuhae & Co.

Preparing for the USM Regime – A Strategic Imperative for Listed Companies. This guidance note, issued by the Institute's Securities Law and Regulation Interest Group (12th issue), was authored by Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Securities Law and Regulation Interest Group members are Stephanie Chan (Chairman), Bill Wang FCG HKFCG, CK Low FCG HKFCG, CK Poon FCG HKFCG, Dr David Ng FCG HKFCG and Tommy Tong FCG HKFCG.

The Protection of Critical Infrastructures (Computer Systems) Bill – An Overview for Governance Professionals. This Technology Interest Group guidance note (17th issue) was authored by Dylan Williams FCG HKFCG and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Institute's Technology Interest Group members are Dylan Williams FCG HKFCG (Chairman), Ricky Cheng, Harry Evans, Gabriela Kennedy and Philip Miller FCG HKFCG.

May

Virtual Asset Staking – Raising Governance Professional's Awareness. The Institute's Technology Interest Group issued a two-part guidance note (18th and 19th issues) to update governance professionals on the comprehensive regulatory framework for virtual asset staking. This was authored by Dylan Williams FCG HKFCG and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Technology Interest Group members are Dylan Williams FCG HKFCG (Chairman), Ricky Cheng, Harry Evans, Gabriela Kennedy and Philip Miller FCG HKFCG.

Whistleblowing – The Software and the Hardware to Thrive. This guidance note, issued by the Institute's Ethics, Bribery and Corruption Interest Group (15th issue), was authored by Dr Brian Lo FCG HKFCG and

Guidance note roundup (continued)

Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Ethics, Bribery and Corruption Interest Group members are Dr Brian Lo FCG HKFCG (Chairman), Cynthianna Yau, Mary Lau, Michael Chan, Ralph Sellar and William Tam ACG HKACG.

June

NGOs and Governance Professionals' Contributions. The Institute's Public Governance Interest Group issued a four-part guidance note (13th, 14th, 15th and 16th issues), authored by April Chan FCG HKFCG and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Public Governance Interest Group members are April Chan FCG HKFCG (Chairman), Lau Ka Shi BBS FCG HKFCG, Margaret Yan, Rachel Ng ACG HKACG and Vicky Li.

Redomiciliation Regime for Hong Kong (Second Update). The Institute's Company Law Interest Group issued a two-part guidance note (13th and 14th issues), authored by Benita Yu FCG HKFCG, Senior Partner, Hong Kong, and Lisa Chung, Partner, Slaughter and May, with contributions from Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Company Law Interest Group members are Benita Yu FCG HKFCG (Chairman), Angela Mak FCG HKFCG, Cathy Yu FCG HKFCG and Wendy Yung FCG HKFCG.

Digitalisation and Competition Law Overview. The Institute's Competition Law Interest Group guidance note (18th issue) was authored by Natalie Yeung, Partner, and Michael Law, Associate, Slaughter and May, and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Competition Law Interest Group members are David Simmonds FCG HKFCG (Chairman), Adelaide Luke, Alastair Mordaunt, Brian Kennelly KC, Mike Thomas and Natalie Yeung.

August

Supporting Digital Investigations – A Practical Primer for Governance Professionals. This guidance note, issued by the Institute's Technology Interest Group (20th issue), explores how governance professionals can play a constructive role in digital investigations. This was authored by Dylan Williams FCG HKFCG and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive, with contributions from Devin Teo and Ivy Chow FCG HKFCG(PE). The Technology Interest Group members are Dylan Williams FCG HKFCG (Chairman), Ricky Cheng, Harry Evans, Gabriela Kennedy and Philip Miller FCG HKFCG.

September

Practical Governance and Compliance Priorities for Directors. This HKCGI guidance note, which draws on insights from the Institute's Director Training Series and outlines 10 practical governance priorities for boards to enhance compliance and avoid common pitfalls, was authored by Gill Meller FCG HKFCG(PE), International Vice President and Institute Past President.

Governance Considerations under Hong Kong's New Regulatory Regime for Stablecoins (Parts 1, 2 and 3). This three-part guidance note (21st, 22nd and 23rd issues), issued by the Institute's Technology Interest Group, was authored by Vincent Chan, Lydia Kung Sen and Vivian Chan, with contributions from Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive. The Technology Interest Group members are Dylan Williams FCG HKFCG (Chairman), Ricky Cheng, Harry Evans, Gabriela Kennedy and Philip Miller FCG HKFCG.

The Institute would also like to thank Michael Ling FCG HKFCG, Chairman of the Institute's Technical Consultation Panel, for his oversight of the Institute's guidance notes, and Mohan Datwani FCG HKFCG(PE), Institute Deputy Chief Executive, who serves as Secretary of the Institute's Interest Groups and is Contributing Editor of the Institute's guidance notes.

Comments and suggestions are welcome, and should be sent to: mohan.datwani@hkcgi.org.hk.

Outstanding media

Website development

Advertisement design

Content marketing

Corporate newsletters

Sales brochures

Professional magazines

ninehills media

T: +852 3796 3060

E: enquiries@ninehillsmedia.com

W: www.ninehillsmedia.com

What directors should know about regulators' disciplinary trends

Jenny WY Yu, Partner, and Raymond NH Chan, Partner, Johnson Stokes & Master, analyse four recent Exchange and SFC disciplinary cases, highlighting a tightening regulatory focus on directors' accountability, due diligence and internal controls.

Directors of listed companies are held accountable to a high standard of ultimate responsibility for the company.

Published findings of disciplinary action taken by The Stock Exchange of Hong Kong Limited (the Exchange) in 2024 and 2025 underline that directors are expected to exercise independent judgement and ensure robust corporate governance with effective internal controls.

As demonstrated by the following case studies, the disciplinary trends show that directors cannot simply absolve themselves of responsibility by relying on other board members or even external professionals.

Case 1: sanctioned for failing to question a sevenfold increase of land valuation in six months

Background

In January 2018, Wisdom Wealth Resources Investment Holding Group Ltd (Wisdom Wealth) announced the acquisition of land in Zhanjiang and engaged a professional valuer to assess its market value.

The value of the land had varied significantly within a year of the acquisition. It was initially valued at RMB1.15 billion in December 2017. However, by 30 June 2018, the valuation had dramatically increased, to RMB8 billion, and then decreased to RMB3.1 billion as of 31 December 2018.

Despite the sevenfold increase in the land's value within six months in early 2018, the directors did not take adequate steps to ensure that their reliance on the valuer's valuation was reasonable.

They failed to seek clarification from the valuer regarding the substantial increase in value, did not consult Wisdom Wealth's auditor and did not consider obtaining a second opinion or other professional advice.

This lack of due diligence and failure to properly discharge their duties led to misleading financial disclosures.

Result

The Exchange took disciplinary action against Wisdom Wealth and its directors, criticising 10 of its directors for their failure to ensure the reasonableness of their reliance on the valuation.

Additionally, two directors were censured for providing incomplete, misleading and/or deceptive information about the valuation methods during the investigation. The directors were also required to attend 17 hours of training on Listing Rule compliance.

Takeaway

Directors must exercise independent judgement, particularly when relying on external information such as valuations, and must consider whether the information is reasonable and well founded. If there is anything unusual, directors should consider seeking clarification or further professional advice.

Case 2: criticised for negligence in risky acquisitions

Background

Three former directors of National Arts Group Holdings Ltd (National Arts) were found to have breached their fiduciary duties during the approval and execution of two acquisitions involving target companies with property units under construction in Malaysia.

Under the acquisition terms, the vendors and/or their related parties would remain responsible for the target companies' outstanding payment to developers. National Arts made full payment upfront by issuing new shares valued at HK$108.8 million as consideration to the vendors.

Highlights

- regulators' disciplinary trends in 2024 and 2025 show a clear emphasis on directors' responsibility, even when professional valuers or advisers are involved
- directors who fail to question irregular valuations, assess acquisition risks or challenge management decisions face censure and mandatory compliance training
- regulators expect boards, including the INEDs, to maintain strong internal controls and ensure transparency in material decisions and use of proceeds

The acquisitions were expected to yield a decent business return, but involved significant risks. The vendors and their related parties failed to pay the developers and ultimately none of the property units were delivered to National Arts.

Result
The Exchange criticised the three former directors for their failure to exercise reasonable skill, care and diligence in safeguarding National Arts' interests. They should have been aware that the acquisitions involved major risk, including that if the vendors failed to make payment, the project may not be completed.

Takeaway
Directors should consider the risks of any proposed acquisition, including the credit risks of any parties responsible for payment.

Case 3: accountability in high-stakes urgent corporate decisions

Background
In a disciplinary action against Fantasia Holdings Group Co, Ltd (Fantasia) and Colour Life Services Group Co, Ltd (Colour Life), the Exchange found significant regulatory breaches.

The case involved the disposal of Colour Life's wholly owned subsidiary, Link Joy Holdings Group Co, Ltd (Link Joy), which was executed without obtaining the necessary shareholders' approval, as is required for a 'very substantial disposal' (VSD). At the material time, Fantasia was the controlling shareholder of Colour Life and was also subject to shareholders' approval for a VSD.

Pan Jun, the former chairman, CEO and executive director of both Fantasia and Colour Life, arranged the disposal to address imminent liquidity concerns.

On 28 September 2021, Colour Life entered into an agreement to sell Link Joy to Country Garden Property Services HK Holdings Co Ltd (Country Garden) for RMB3.3 billion. However, two days later, Colour Life entered into a loan agreement with Country Garden for RMB700 million, which was repayable within a brief period. This loan agreement included terms that allowed Country Garden to request the transfer of Link Joy in the event of certain default conditions.

On 4 October 2021, the default conditions were triggered, leading to the transfer of Link Joy to Country Garden. Mr Pan did not consult the board of directors of either Fantasia or Colour Life before entering into the loan agreement, nor did he disclose the agreement to either of the boards in a timely manner.

When the other directors became aware of the situation, some of them failed to make necessary inquiries or to seek further information about the transaction. Additionally, they did not question Mr Pan's conduct, including his decision to keep the arrangement to himself, disregarding the companies' internal control policies.

Result
The Exchange issued a Prejudice to Investors' Interests Statement against Mr Pan, indicating that his continued involvement in the companies could harm investor interests. Additionally,

> "the disciplinary trends show that directors cannot simply absolve themselves of responsibility by relying on other board members or even external professionals"

the other directors who did not question Mr Pan's actions were censured and directed to undergo 15 to 18 hours of training on Listing Rule compliance.

Takeaway
Directors should actively voice their views and concerns, particularly if they become aware that another member has withheld information or has failed to comply with internal controls.

Case 4: beware the consequences of bypassing board approval

Background
The Securities and Futures Commission (SFC) and the Exchange took enforcement action against FingerTango Inc (FingerTango) and its former directors, including independent non-executive directors (INEDs).

The case related to a policy adopted by all directors, which allowed certain investment decisions to bypass board approval. This policy led to a series of problematic investments and loans,

> these recent disciplinary cases show a regulatory trend focusing on enhancing and strengthening internal controls, as well as holding directors accountable for inadequate internal controls

resulting in substantial financial losses for the company.

FingerTango, a company that had been listed on the Main Board of the Exchange since July 2018, raised net proceeds of HK$967 million from its initial public offering. Shortly after listing, the company invested HK$450 million of these proceeds in an unlisted wealth management product without the board's knowledge.

This investment deviated from the intended use of proceeds as stated in the company's prospectus, which had indicated that any unused proceeds would be placed in short-term demand deposits or money market instruments. The company did not disclose this change in the use of proceeds in its prospectus or subsequent announcements, violating several listing rules.

In December 2019, FingerTango partially redeemed the fund and immediately invested another HK$250 million in loan notes issued by a small-scale private company. This investment resulted in a loss of HK$258.75 million, including accrued interest, due to a default on the loan notes.

Between May 2020 and March 2021, FingerTango and its subsidiaries subsequently entered into 20 loan agreements with 15 borrowers, totalling over HK$500 million. These loans were largely unsecured and interest-free, leading to an impairment loss of approximately HK$424 million, with over 80% of the loans in default.

Result

The SFC's investigation showed that the directors failed to carry out proper procedures and due diligence before entering into these loan agreements. Hence, the SFC commenced legal action seeking disqualification and compensation orders against the former directors, holding them accountable for the losses incurred by the company and its subsidiaries.

Takeaway

Directors, including INEDs, should ensure there is a robust corporate governance system in place, with adequate internal control policies and procedures that are properly implemented. They cannot simply absolve themselves by adopting a loose policy – and they should ensure they are involved in the material decision-making processes of the company.

Concluding remarks

These recent disciplinary cases show a regulatory trend focusing on enhancing and strengthening internal controls, as well as holding directors accountable for inadequate internal controls.

Directors are expected to exercise independent judgement and to consider material risks when approving company transactions or acquisitions. It is insufficient to simply rely on other board members or external information.

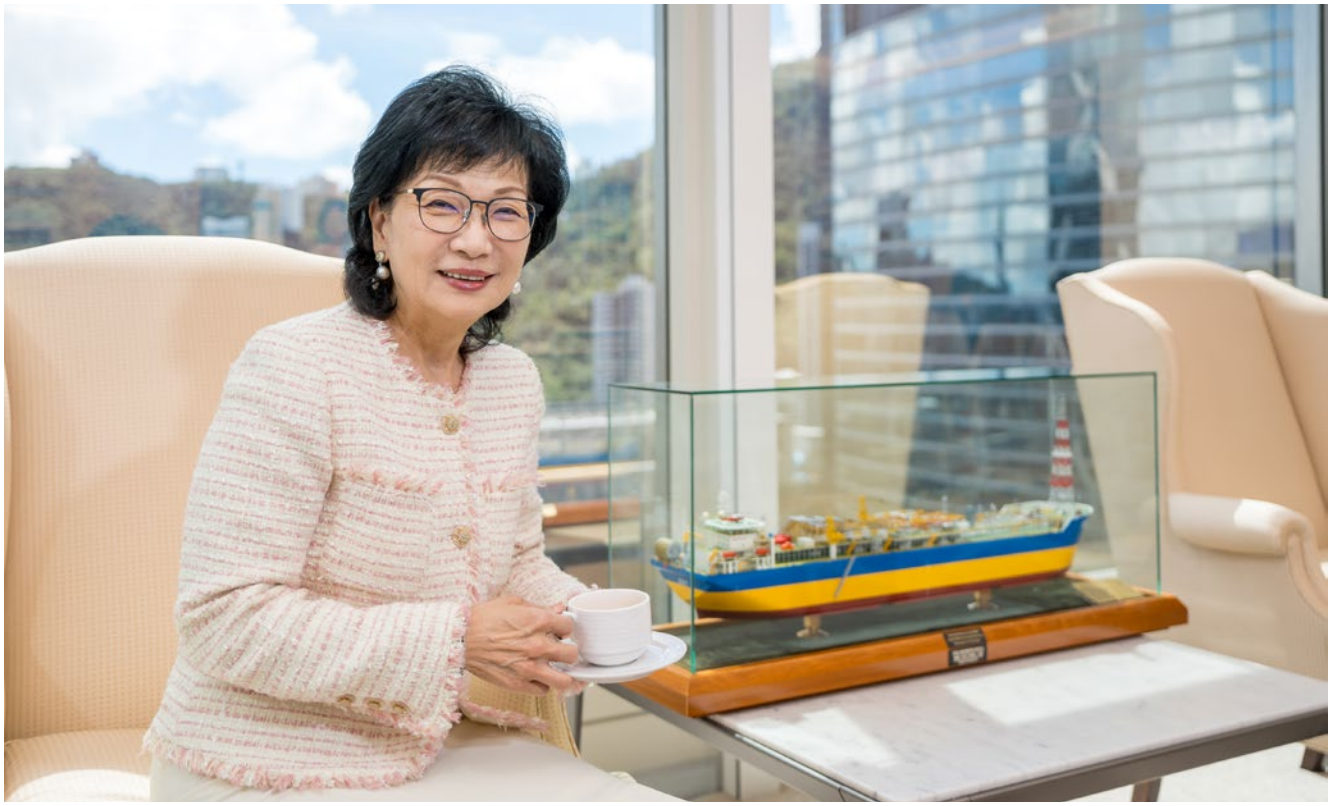
This demonstrates a focus on corporate governance controls to maintain investor confidence in Hong Kong listed companies.

Jenny WY Yu, Partner, and Raymond NH Chan, Partner

Johnson Stokes & Master

Edith Shih FCG(CS, CGP) HKFCG(CS, CGP)(PE)

Honorary Adviser to Council, Past International President and Institute Past President, and Executive Director and Company Secretary, CK Hutchison Holdings Ltd



How and when did you first get involved with the Institute? And what was your professional position at the time?

'I became Company Secretary of Hutchison Whampoa in 1997, which marked the beginning of my involvement with the Institute. At that time, there was a panel known as the Company Secretaries Panel – now the Governance Professionals Panel – which still meets four times a year. Three of the meetings were attended by key regulators, while the fourth was reserved for internal discussions among panel members. I served on this panel from 1998 and was its Chair from 2012 to 2018. Our members came from a wide range of industries – banking, property, insurance and SMEs. In 2004, I became a Fellow of the Institute and later served as Vice-President, then President. I joined the International Council in 2014, serving as International Vice President for four years and International President for two.'

You remain very active in the Institute. What is your role at the moment?

'I currently serve as Honorary Adviser to Council. As I grow older, I've come to realise that while one can always help, one must also know when to step back. These days, I mostly observe and offer advice and assistance when needed. If I feel that the Institute is heading in the wrong direction, or if support is required, I will step in. Otherwise, I'm more involved in informal ways, such as helping to arrange the booking of venues for major events, or to assist with organising and inviting speakers for signature Institute events. After stepping down as International President, I continued to serve as the Hong Kong/China representative on the International Council and also continued to attend Institute Council meetings to keep apprised of its progress. So from that perspective, I could share insights with both Councils on their respective approaches.'

What aspect of the Institute's activities and initiatives inspire and engage you the most?

'For several years now, I've devoted more time to nurturing the next generation. As early as 2006, our company began taking on interns from the Institute each year, which we still do. I also serve as a mentor and some of my mentees still stay in touch with me – many have now become senior

professionals in their fields. In recent years, with the support of the Institute, my interns have been featured as speakers at a webinar we hold toward the end of their summer internship. We choose an emerging governance topic of interest, research the topic, prepare power point slides, write up a script and conduct a webinar. This summer, we focused on the upcoming Uncertificated Securities Market regime in Hong Kong. Together, we studied the regulations and reached out to the SFC, HKEX and registrars to gain a first-hand understanding. When one studies legislation closely, one often spots issues that even the regulators may not have considered while drafting the legislation. That kind of intellectual exchange benefits both students and professionals, creating a life-long learning experience, which they treasure. Our most recent webinar attracted over 2,000 registrations.'

Why do you feel giving back is important?

'I feel very blessed in my life. My parents were originally from Fujian and came to Hong Kong with little, but decided to settle. I was born and raised here and, when I look back, I realise how smooth my life has been compared with many of my friends and relatives. I've never truly faced serious hardship, and that makes me feel all the more responsible to help others.

In later life, I truly believe we should spend more time giving back, if we can. Over the years, I've set up scholarships, sponsored students, mentored young professionals, looked after the elderly and stayed active in my alma mater's alumni association. I sometimes feel students and young professionals don't always know how to make the most of such opportunities – they should learn to use these connections and networks wisely, because professionals like us can give them a hand and open doors for them. That kind of help often lasts far longer and has a more substantive impact than does pure financial support.'

Over the years, many individuals have contributed behind the scenes to the Institute's growth. From your perspective, how have the efforts of these volunteers shaped the Institute's development and success?

'At the Institute, we have many colleagues who are very committed to the organisation. Despite their busy schedules, they still make time to serve and that dedication is admirable. Volunteering takes many forms – some help with membership, examinations or qualifications, while others join academic or technical panels to write or review papers. Many also serve as mentors or take part in the Mentorship and Student Ambassador programmes for university students. These long-serving volunteers form the backbone of the Institute's development.'

> "governance is not merely about compliance or best practices, it's also about a moral and ethical mindset"

Could you tell us a little about your personal philosophy or guiding principles for both your professional and personal life?

'Whatever you do, give it your all and do it to the best of your ability. Some people say I take things too seriously – even when parking my car, I'll make sure to get it straight. But I believe that if you are not rigorous with yourself, you cannot expect high standards from others. At a speech I gave at my former school, a younger alumna recalled something I once said, that doing something 100% is not enough. If one performs at 100%, one's subordinates might reach 80%, and their juniors perhaps 60%. To lead others to excellence, one must strive to go beyond perfection.'

What value do you believe governance brings to organisations and the wider society, and how does the Institute contribute to that?

'To me, governance is not merely about compliance or best practices, it's also about a moral and ethical mindset. An organisation guided by integrity and conscience not only ensures compliance, but also allows its people to carry that mindset into their family life, social circles and professional communities. This in turn nurtures a more ethical society and, hopefully, a better world. Our role is to pass on this torch of governance. In fact, we once had a programme called Passing the Torch, which I initiated years ago. It involved university students visiting secondary schools to introduce the concept of corporate governance. Although that programme has since ended, its spirit of passing on the value of governance to the next generation remains.'

施熙德女士 FCG(CS, CGP) HKFCG(CS, CGP)(PE)

公会理事会荣誉顾问、国际公会前会长及公会前会长、长江和记实业有限公司执行董事兼公司秘书

您最初是如何、又在何时开始参与公会工作的？当时的职务是什么？

‘我在 1997 年成为和记黄埔的公司秘书，这是我与公会开始接触的契机。当时公会设有一个名为 (Company Secretaries Panel) 的小组（现称 Governance Professionals Panel），现在仍每年召开四次会议，其中三次邀请主要监管机构出席，另一次则由小组成员内部交流。我自1998年起成为小组成员，并于2012年至2018年担任主席。小组成员来自银行、地产、保险、中小企业等多个行业。2004 年，我成为公会资深会士，先后担任副会长、会长。2014 年，我加入国际理事会，并担任国际副会长四年、国际会长两年。’

您至今仍非常积极参与公会事务，目前担任何种角色？

‘现在我是公会理事会的荣誉顾问。年纪渐长，我逐渐体会到虽然我们总可以帮忙，但也要懂得何时该退后一步。所以我现在主要是观察并提供意见和援助，如果觉得公会的方向有偏差，或需要支持时，才会介入，否则多以非正式的方式参与，例如为公会大型活动预订场

地，协助筹办公会的重点会议并邀请演讲嘉宾。卸任国际会长后，我继续担任国际理事会的香港/中国代表；为了充分了解香港公会的情况，我也继续参加香港的理事会会议。因此，从这个角度来看，我可以向两个理事会分享各自的观点和方针。

公会的哪些工作或活动最令您投入或受到启发？

‘近年来，我更专注于培育下一代。早在 2006 年，我们公司便开始每年聘请来自公会的实习生，至今仍是这样做。我也担任导师，有些学员至今仍和我保持联络，他们当中许多现在已是业界的资深专业人士。近年来，在公会的支持下，我的实习生在暑期实习结束前的网络研讨会上担任演讲嘉宾。我们选择一个新兴的治理议题，进行相关研究，准备概要介绍，撰写讲稿，并主理研讨会。今年夏天，我们的主题是香港即将推行的无纸证券市场规定。我们一起研读法规，并走访证监会、联交所和股份过户登记公司，亲身了解制度运作。在深入研究法规的过程中，常能发现连监管机构在起草立法时都可能未必想到的问题。这种思想交流对学生与专业人士都有益处，为他们带来珍贵的终身学习体验。最近的一场研讨会有超过 2,000 人报名。’

为什么回馈社会对您如此重要？

‘我一直觉得自己很有福气。我的父母是福建人，几乎一无所有来到香港，在此落地生根。我在香港土生土长，现在回头看，发觉自己的人生旅程比许多亲戚朋友都顺遂得多。我从未真正经历过困苦，这更让我觉得有责任帮助别人。

在人生后半段，我坚信如果我们有能力，应该花更多时间回馈社会。这些年来，我设立了奖学金、资助过学生、指导年轻专业人士、关顾长者，也积极参与母校校友会的事务。有时候我觉得，学生和年轻专业人士未必懂得如何善用机会。其实他们应该运用人脉和网络，因为像我们这样的专业人士确实能帮他们一把，为他们打开大门。这种帮助的作用往往比金钱资助更为长久，也更有实质性的影响。’

多年来，许多人默默付出，推动了公会的发展。从您的角度来看，这些志愿者的努力如何塑造了公会的发展与成功？

‘我身边也有不少同事积极参与公会事务，虽然工作繁忙，仍愿意抽时间服务公会，这种精神非常难得。公会的义务工作形式多样，有些人参与会籍事务、考试与资格制度，有些加入学术或技术小组，撰写或审阅文章，也有不少人担任导师，或加入大学生导师及大使计划。这些长期投入的义工是公会发展的基石。’

> **“良好的治理不只是遵守法规或採纳最佳做法，更重要的是道德与伦理的思维模式”**

您的人生与工作哲学或原则是什么？

‘无论做什么事都要全力以赴、做到最好。有人说我太认真，连停车也会反复调整，确保停得正正直直。但我始终相信，如果你对自己都不严谨，就无法对别人有要求。有一次我在母校演讲，一位年轻校友提到我说过的一句话 — 做到 100% 是不够的。因为你做到 100%，你的下属大概只做到 80%，而他们的下属可能只做到 60%。若想带领他人追求卓越，就必须超越完美。’

您认为良好的治理对机构与社会有何价值？公会又如何推动这种价值？

‘我始终相信，良好的治理不只是遵守法规或采纳最佳做法，更重要的是道德与伦理的思维模式。一个组织若能以正直和良知为本，不仅有助合规，更能透过员工，把这种精神带进家庭、社会和专业圈子，从而培养社会的道德意识，为世界带来正向影响。我们的工作，就是传承治理的精神。我当年推动一个名为薪火相传的公会计划，让大学生到中学去介绍公司治理的概念。虽然这计划后来停办了，但它的精神仍在，把治理的价值一代一代传承下去。’

Professional Development

Seminars: September 2025

8 September

Share repurchases in action – transactional uses and governance essentials

Chair: *Frank Yuen FCG HKFCG, Group General Counsel and Head of Compliance, CK Hutchison Holdings Ltd*

Speakers: *Grace Huang, Partner, and Cindy Kwong, Counsel, Freshfields*

17 September

Understanding Hong Kong profits tax – essential insights for company secretaries

Chair: *Wendy Kam FCG HKFCG(PE), Institute Professional Services Panel member, and Managing Director, Corporate Secretarial Services, In.Corp Corporate Services (HK) Ltd*

Speakers: *Philip Hung, Director, Tax Controversy Services, and Felix Tsang, Associate Director, Tax Controversy Services, PwC Hong Kong*

18 September

The backbone of governance – developing and enforcing a code of conduct in organisations

Speakers: *Patricia Hui FCG HKFCG(PE); Christine Cuthbert, Partner, Baker & McKenzie; and Mavis Tan, Partner, Control Risks*

24 September

Trusts uncovered – best practices to avoid costly mistakes

Chair: *Edmond Chiu FCG HKFCG(PE), Institute Council member, Professional Development Committee member, and Professional Services Panel Chair, and Head of Company Secretarial Services, Greater China, Vistra*

Speakers: *Franky Fung, Partner, Sun Lawyers LLP, and Alban Yeung FCG HKFCG, Advisory Director, PAL Advisory Ltd (panellist)*

26 September

CSP training series: notifiable transactions – practice and application

Speaker: *Ricky Lai FCG HKFCG(PE), Company Secretary, China Renewable Energy Investment Ltd*

29 September

CSP foundation training series: directors, secretaries, officers and auditors of Hong Kong private limited companies

Speaker: *YT Soon FCG HKFCG(PE)*

ECPD seminars/Videos on Demand

ECPD training is organised by the Institute to facilitate its members and other governance professionals to acquire governance knowledge, corporate secretarial skills, and related thought leadership and best practices.

In addition to in-person seminars, ECPD training is delivered via live webinars or pre-recorded videos for maximum accessibility and flexibility.

Details of the Institute's forthcoming ECPD seminars and ECPD Videos on Demand are available in the Professional Development section of the Institute's website: www.hkcgi.org.hk.

For enquiries, please contact the Institute's Professional Development Section: (852) 2830 6011, or email: cpd@hkcgi.org.hk.

Membership

New Associates

The Institute would like to congratulate our new Associates listed below.

Au-Yeung Lok To	Chow Man Yee	Leung Nikita Wai Ling	Ng Tsz Lok	Tsang Kwok On
Cai Xiaoting	Ho Chui Shan	Leung Wing Sum	Poon Enoch	Wong Ching Wai
Chan Hiu Kuk	Hui Sin Nga	Lin Baohuan	Shi Jingyi	Wong Kwok Kuen
Chan Hui Yi, Winnie	Jiang Peng	Lin Lam	Shum Ka Fai	Wong Wai Ying
Chan Man Yan	Kwan Ka Ming	Lo Wai Kin, Kent	Siu Wing Shan	Yau Chak Ming
Chan Yuk Ping	Lam Ho Yan	Lung Ka Wa	So Ching Yee	Yu Cassie Chui Ying
Chen Yiwei	Lau On Kei	Man Kwok Leung	Tam Shuk Kwan	Yu Suet Ying
Cheung Yan Ting	Law Tak Lok, Owen	Ng Hing Ho	Tang Jie	Yuen Wing Ki
Cho Yin	Lee Man Hung	Ng Kuen Lai	Tsang Kam Ho	

New graduates

The Institute would like to congratulate our new graduates listed below.

Chan Fuk Wing	Huang Shuwei	Lo Pui Yee	Tsang Yee Wah, Eva	Yip Ying Tung
Chan Hiu Lam	Kwok Wing Nam	Ng Tsz Yan	Tsoi Kwan	Yuen Ka Wai, Kathy
Chan Ka Ka	Lai Hoi Lam	Pang Ho Kin	Wong Jonas Yan-ho	Zhang Tianyuan
Chan See Wun	Lam Yan Kwing	Qiu Zesen	Wong Ka Wo	Zhao Na
Chan Yee Lam	Law Pong Ming	Sung Shing Him, Kevin	Wong Tsz Yu	Zhuang Xiaoqian
Ching Ho Leung	Liu Chuyu	Sze Cynthia	Wong Wing Sum	
Chiu Lok Ching	Liu Yang	Tam Bronson	Yau Sau Ying	
Fung Sin Ting, Karin	Liu Yaojia	Tong Yuen Ki, Melody	Yen Hiu Lui	

Membership (continued)

Membership activities: September 2025

13 September

Summer sports series – bowling fun day

20 September

Mentorship training – promoting DEI and inclusive leadership: a strategic governance approach

22 September

NextGen Group – experiencing ice curling

HKCGI Annual Convocation 2025

The Institute's Annual Convocation was held on 8 October 2025, with welcoming remarks from Guest of Honour Gill Meller FCG HKFCG(PE), International Vice President and Institute Past President, and Stella Lo FCG HKFCG(PE), Institute Vice-President.

In the year 2024/2025, 70 Fellows, 334 Associates and 84 graduates were admitted to the Institute. New Fellows, Associates and graduates, together with awardees of the Institute's Chartered Governance Qualifying Programme (CGQP) module prizes and merit certificates, as well as the HKCGI Foundation scholarships and subject prizes, received their certificates and awards at the convocation.

This year, as a way to express the Institute's gratitude for their long-term support and contributions, those holding membership status for 50 years and over were also invited to join the ceremony.

Certificates were presented by Institute Vice-President Stella Lo FCG HKFCG(PE), Guest of Honour Gill Meller FCG HKFCG(PE), Institute Treasurer Daniel Chow FCG HKFCG(PE), Institute Past President Ernest Lee FCG HKFCG(PE), Institute Past President and Council member David Fu FCG HKFCG(PE), and Council members Robin Healy FCG HKFCG and Matthew Young FCG HKFCG(PE). The Institute also invited Cynthia Lai ACG HKACG to share her experience and aspirations of the profession from the perspective of the younger generation.

Advocacy

CGI's AGM 2025 and Council meeting

On 9 September 2025, The Chartered Governance Institute (CGI) held its annual general meeting (AGM) in Sydney, followed by its Council meeting on 10 and 11 September 2025.

Edith Shih FCG (CS, CGP) HKFCG(CS,CGP)(PE), Honorary Adviser to Council, Past International President and Institute Past President, Gill Meller FCG HKFCG(PE), International Vice President and Institute Past President, and Ellie Pang FCG HKFCG(PE), Institute Chief Executive, attended the AGM and Council meeting as representatives of the Institute.

The Institute welcomes the governance initiatives outlined in the 2025 Policy Address

The Institute warmly congratulates Chief Executive John Lee on his 2025 Policy Address, which strengthens accountability, transparency and oversight across public administration and corporate governance. The Institute fully supports these initiatives, which enhance Hong Kong's competitiveness as a trusted, globally connected international financial centre.

Additionally, under the forthcoming Jockey Club HKCGI Sports Governance Programme, the Institute will assist the National Sports Association in strengthening their governance practices to develop a robust sports governance ecosystem aligning with the Policy Address.

Research report on risk management and internal control systems (RMIC)

On 25 September 2025, the Institute published a joint research report with KPMG, titled Enhancing Accountability: Revised Corporate Governance Code on Risk Management and Internal Control Systems – Four Essential Questions for Directors to Ask & Answer.

The report provides practical guidance for boards and management on implementing effective RMIC reviews. It offers a comparative analysis of disclosure requirements in other major markets and demonstrates Hong Kong's commitment to advancing good corporate governance practices in RMIC.

For details, download the full report from the Research Papers page under the Thought Leadership section of the Institute's website: www.hkcgi.org.hk.

Celebrating the Mid-Autumn Festival

To celebrate the Mid-Autumn Festival, the Institute ordered mooncakes, as well as snack packages from Gingko House Bakery, for the Secretariat staff in Hong Kong. Gingko House Bakery is a social enterprise dedicated to promoting senior employment, which provides Hong Kong with delicious handmade treats. Similar arrangements were made for the staff members of the Institute's Beijing Representative Office.

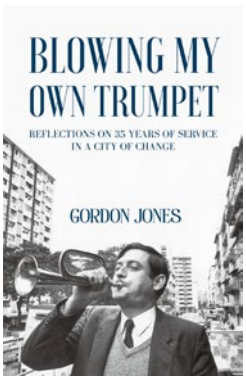
The Education Bureau's Business-School Partnership Programme's 20th Anniversary Commemoration cum Certificate Presentation Ceremony

The Institute has partnered with the Education Bureau's Business-School Partnership Programme (BSPP) to strengthen its engagement with the secondary education sector.

On 19 September 2025, the Institute was honoured to be represented by Melani Au ACG HKACG, Director and Head of Membership Development, at the BSPP's 20th Anniversary Commemoration cum Certificate Presentation Ceremony. The Institute looks forward to further collaboration with schools and community partners to cultivate a greater interest in governance and to support the development of future professionals.

Blowing My Own Trumpet by Gordon Jones

Gordon Jones FCG HKFCG, a long-standing Fellow of the Institute and the recipient of the HKCGI Prize in 2016, published his book, *Blowing My Own Trumpet*, on 1 November 2025. In this memoir, Gordon reflects on his 34-year career in the Hong Kong Government, where he held a variety of senior positions within the Administrative Service. The book also delves into his contributions to the revision of Hong Kong's company law, including initiating the rewrite of the Companies Ordinance, which began in 2006, and the reform of corporate governance.



Chartered Governance Qualifying Programme (CGQP)

November 2025 examination diet

Examination admission slips, together with the Instructions to Candidates, were released on 28 October 2025. All candidates are reminded to follow the instructions before taking the examinations.

Candidates who are unable to attend the scheduled CGQP November 2025 examinations may apply for an examination postponement by submitting a relevant medical certificate and/or supporting document(s). All applications must be submitted to the Institute on or before Thursday 18 December 2025.

Key dates

Key dates	Description
18 December 2025	Closing date for examination postponement applications
Late February 2026	Release of examination results
Late February 2026	Release of examination papers, mark schemes and examiners' reports
Mid-March 2026	Closing date for examination results review applications

Note: The Institute reserves the right to change the dates and details without prior notice.

For details, please visit the Examinations page under the Chartered Governance Qualifying Programme subpage of the Studentship section of the Institute's website: www.hkcgi.org.hk.

For enquiries, please contact the Qualifications and Assessments Section: (852) 2830 6010, or email: exam@hkcgi.org.hk.

Forthcoming studentship activities

Date	Time	Event
29 November 2025	11.00am–2.00pm	Student Ambassadors Programme: tea reception

Promoting the governance profession to university students

The Institute continues to work closely with universities to encourage more young people to consider governance as a career. In collaboration with the following universities, the Institute arranged a number of career and promotional talks for their respective students between September and November 2025.

The Institute would like to extend its heartfelt thanks to all Institute members who generously shared their time, insights and professional experience with the university students during the recent career and promotional talks (in alphabetical order of surname):

Melani Au ACG HKACG
Mohan Datwani FCG HKFCG(PE)
Patricia Hui FCG HKFCG(PE)
Emily Ng ACG HKACG
Ellen Suen ACG HKACG
Matthew Young FCG HKFCG(PE)

Date	University
30 August	Hong Kong Baptist University
1 September	Hong Kong Metropolitan University
29 September	Hong Kong Metropolitan University
2 October	Saint Francis University
6 November	The University of Hong Kong
7 November	City University of Hong Kong
10 November	Hong Kong Shue Yan University

Hong Kong's blueprint for intellectual property

Each year, the Chief Executive's Policy Address outlines the Hong Kong SAR Government's priorities and reform agenda, offering valuable insights into the city's evolving economic strategy and regulatory direction.

In his Policy Address this year, Chief Executive John Lee placed strong emphasis on intellectual property (IP) as a key pillar of innovation and technology (IT) development. Hong Kong's global ranking in IP rights has risen to sixth place, underscoring the city's growing strength in protecting and managing intangible assets such as inventions, creative works and scientific discoveries.

Building on this momentum, the government aims to further position Hong Kong as a leading regional IP trading hub. The 2025 Policy Address introduced new initiatives to enhance IP financing, valuation and protection – key enablers for commercialisation and cross-border IP transactions. The principal measures proposed in this Policy Address are outlined below.

IP financing sandbox

To unlock the commercial potential of intellectual property, the government will introduce an IP financing sandbox, jointly developed by the Commerce and Economic Development Bureau, the Intellectual Property Department and the Hong Kong Monetary Authority.

Targeting the technology sector, the sandbox will allow startups and small and medium-sized enterprises (SMEs) to use their IP assets, such as patents and copyrights, as collateral for financing. By integrating expertise from banking, insurance, valuation and legal professionals, the initiative is designed to create a supportive environment for IP-backed lending. In addition, a subsidy scheme for patent valuation will be launched to help smaller IT enterprises access credit more easily and turn their innovations into growth opportunities.

Patent and trademark support

By the end of 2025, the Hong Kong Technology and Innovation Support Centre will begin operations to provide patent evaluation services aligned with national standards. To help IT-related SMEs secure financing, the government will also launch a two-year pilot programme to subsidise patent valuation. These measures are intended to give innovative companies reliable references for credit assessment, reduce financing barriers and facilitate the commercialisation of their patented technologies.

Protecting copyright

The government is moving to modernise Hong Kong's IP framework to keep pace with technological advances, particularly in artificial intelligence (AI). Following a public consultation on updating the Copyright Ordinance, a code of practice will be developed and legislative amendments will be introduced to strengthen protection for AI-related creations. In parallel, a review of the registered designs regime will be conducted, with consultation expected by the end of the year. The purpose of these reforms is to ensure that Hong Kong's IP laws remain agile, forward-looking and aligned with international standards in safeguarding innovation.

Promotion

To further enhance Hong Kong's profile as a regional IP trading hub, the government will step up international promotion and recognition efforts. In partnership with the Hong Kong Trade Development Council, IP financing and trading opportunities will be showcased at the Business of IP Asia Forum 2025, to be held on 4 and 5 December at the Hong Kong Convention and Exhibition Centre. The Intellectual Property Department will also continue to nominate outstanding local enterprises for the prestigious China Patent Awards, coorganised by the China National Intellectual Property Administration and the World Intellectual Property Organization. These initiatives aim to highlight Hong Kong's strengths in IP protection, encourage cross-border collaboration and open new channels for businesses to monetise their innovations.

Labuan IBFC
International Business and Financial Centre, Malaysia

LABUAN IBFC
ASIA'S PREMIER INTERNATIONAL FINANCIAL HUB

Labuan International Business and Financial Centre (Labuan IBFC), located off the North West coast of Borneo, offers global investors and businesses the benefits of being in a well-regulated jurisdiction that provides fiscal, legal and currency neutrality, in addition to being an ideal location for cost-efficient substance creation.

Labuan IBFC is a wholesale financial, risk and wealth management intermediation centre that also boasts a wide range of business structures including solutions for fintech or digital businesses. It is also home to the world's first sukuk and is acknowledged as an Islamic financial hub.

Well-supported by a robust, internationally recognised yet business-friendly legal framework, Labuan IBFC operates within comprehensive legal provisions and guidelines, enforced by a single regulator, Labuan Financial Services Authority – a statutory body under the Ministry of Finance, Malaysia.

Labuan, also known as the 'Pearl of Borneo', offers a myriad of business and leisure opportunities. It is also a hub for financial tourism as its excellent location and compact structure offer easy connectivity between the financial district, and nature offerings.

Labuan IBFC Inc. Sdn. Bhd. (817593-D)
Suite 3A-2, Level 2, Block 3A,
Plaza Sentral, Jalan Stesen Sentral,
KL Sentral, 50470 Kuala Lumpur, Malaysia
Tel: +603 2773 8977
Fax: +603 2780 2077
Email: info@LIBFC.com
@LabuanIBFC
Labuan IBFC

www.LABUANIBFC.com

GO

BEYOND

Meet our all-new long-distance leader. Reaching 8,000 nm/14,816 km[1] at Mach 0.85, the Gulfstream G800™ takes you farther faster, guided by the award-winning Symmetry Flight Deck.

Gulfstream™

A General Dynamics Company

[1]NBAA IFR theoretical range at Mach 0.85 with 8 passengers, 4 crew and NBAA IFR reserves. Actual range will be affected by ATC routing, operating speed, weather, outfitting options and other factors. All performance is based on preliminary data and subject to change.