WBY LAWYERS
王斌逸律師事務所

BRIEFING

Summary of the SFC Circular to Licensed Corporations – Use of Generative AI Language Models (12 Nov 2024)[1]

Language models ("LMs")[2] are a type of generative artificial intelligence that uses machine learning to generate text that resembles human language based on the large amount of training data input. Common use cases include content creation and chatbots. As LMs becomes more accessible, financial institutions have increasingly adopted LMs in both their internal and client-facing operations to improve efficiency as they rely on artificial intelligence-generated content in their investment research, advisory and decision-making and client interaction functions. To address the relevant risks arising from and supervise the financial sector's adoption of LMs, the global regulatory direction appears to have taken a risk-based approach.

The European Union (the "EU") has recently enacted the EU Artificial Intelligence Act covering all types of artificial intelligence systems across a broad range of industries and sectors. The EU Artificial Intelligence Act introduces a risk-based framework and categorises artificial intelligence systems into three tiers based on the level of risk these systems pose to user rights and safety. Artificial intelligence systems used in connection with creditworthiness and risks assessments as well as critical financial infrastructure are considered as high-risk and are thus subject to strict requirements covering risk mitigation measures, demands for high-quality datasets, and human oversight.

On the other hand, the US has not yet enacted any overarching artificial intelligence-specific legislation but focuses on addressing the risks of adopting LMs through existing regulations. There have been various initiatives from US regulators to manage artificial intelligence-related risks in the financial sector under existing federal securities laws, targeting the development and adoption of LMs by investment advisers and their relevant policies and procedures.

Like the US, various regulators in Hong Kong have been taking steps to provide sector-specific guidance within the existing frameworks regarding governance of the use of LMs as Hong Kong, and its financial institutions in particular, have shown great enthusiasm in the use of LMs in their businesses and services.[3] The Financial Services and the Treasury Bureau's (the "FSTB") statement in October 2024[4] set out the Government's risk-based policy on the responsible application of LMs in the city's finance industry, which encourages the industry to embrace the new technology while emphasising the importance of risks mitigation. Prior to the FSTB's statement, the Insurance Authority (the "IA") already published an article in May 2023 about using LMs in chatbots in connection with handling insurance claims. The article addressed the risks of such use of LMs and stated that the IA would likely apply its current

regulatory standards and principles as a starting point.[5] Similarly, the Hong Kong Monetary Authority (the "HKMA") focuses on enhancing risk management, system integration, continuous monitoring and customer experience in the banks' use of LMs for customer interaction, assessments, predictions, analytics and decision-making. In August 2024, the HKMA issued a circular which furnished a list of guiding principles for banks' use of LMs in customer-facing applications from a consumer protection perspective.[6] And in September 2024, the HKMA further published a comprehensive research paper[7] which provides an "indicative roadmap" for banks to integrate LMs into their operations and even launched the Generative Artificial Intelligence (GenA.I.) Sandbox initiative for banks.[8]

As the regulator of a major international financial market, the Securities and Futures Commission of Hong Kong (the "SFC") has issued a circular on 12 November 2024 (the "Circular")[9] which outlines its risk-based approach to the responsible adoption of LMs by Licensed Corporations (the "LCs"). The Circular addresses the use of LMs by LCs specifically in carrying out their regulated activities, rather than the use of AI generally or the use of LMs in non-regulated activities (such as the use of AI in KYC or client on-boarding process generally). This article provides an overview of the SFC's regulatory framework for LCs' adoption of LMs, which focuses on supervising the deployment of LMs under the existing Hong Kong financial regulatory regime.

Risks associated with the adoption of LMs by financial institutions

The Circular highlights several risks associated with the LCs' use of LMs and echoes the risks identified by the HKMA and the IA. The most significant risks relevant to individual LCs and the financial services sector's LM integration are summarised as follows:

1. Operational risks: Failure or malfunctioning of LMs may lead to disruptions to financial services provided by LCs, whereas inaccurate or inappropriate data inputs and outputs may lead to operational and systemic challenges such as producing wrong or misleading information and perpetuating biases that result in inadequate financial advice or decisions;

2. Reputational risks: Failure or misuse of LMs may damage the reputation of financial institutions; and

3. Legal and security risks: There will be heightened cybersecurity vulnerability, which may lead to data protection and privacy breaches, confidentiality issues, and other compliance issues.

Risk management and mitigation

To address the abovementioned risks, the SFC has adopted an approach similar to the US and focuses on addressing risks through existing regulations. The Circular sets out how LCs should manage and mitigate risks in adopting LMs in proportion to the materiality of the impact and the level of risk in relation to a specific use case under the existing regulatory regime.

Core Principle 1: LM risk management

Generally, the SFC expects LCs to conduct model testing and validation, model performance assessment as well as tests on cybersecurity and data risk management controls before adopting LMs, and subsequently conduct ongoing review and monitoring of the performance of LMs to ensure that they remain fit for purposes and continue to function properly under changing market circumstances. LCs are also expected to keep proper documentation of such model testing, validation and ongoing review and monitoring.

In particular, the use of LMs for providing investment recommendations, advice or research to clients are considered by the SFC as high-risk use cases because inadequate use of LMs in this respect may result in misinformation and financial product suitability issues. These use cases necessitate the following risk management measures:

1. LCs should conduct model validation, ongoing monitoring and review on the adoption of LMs, including testing output robustness, to ensure accuracy;
2. LCs should incorporate human oversight when using LMs to review outputs generated by LMs and to ensure factual accuracy; and
3. LCs should maintain a high level of transparency with clients about the use of LMs by continuously making disclosures whenever the clients interact with LMs.

In addition, if LCs engage in the development of LMs, LCs must ensure functional independence. LCs must also segregate model development activities from the functions that conduct model validation, ongoing monitoring and review.

Core Principle 2: Cybersecurity and data risk management

LCs should implement cybersecurity policies, procedures and internal controls to identify and address attacks against LMs and protect sensitive and confidential data, including personal data and data for training the LMs. Furthermore, LCs are expected to ensure the quality of the data for training the LMs to avoid biases.

Core Principle 3: Third party provider risk management

Where LCs rely on LMs provided by a third party, they should exercise due skill, care and diligence in selecting such third party and conduct ongoing monitoring of the third party to assess whether the third party has the requisite expertise and has effective model risk management framework concerning the LC's specific use cases of LMs. Moreover, the above core principles equally apply to each third-party component of the LC's LM as an LC is expected to allocate responsibilities between itself and the third party in risk management and control. Depending on the LC's dependence on third party LMs, LCs should establish contingency plans to prepare for any operational failures.

Core Principle 4: Senior management responsibilities

To effectively comply with the Core Principles above, LCs should implement policies, procedures and internal controls for using LMs, including establishing clear lines of

accountability and adequate senior management oversight. LCs should also train its staff in the business, technology, risk, and legal and compliance functions to ensure they are aware of the capabilities, risks and limitations of LMs and are competent in effectively using LMs in the relevant use cases while effectively managing risks and maintaining regulatory compliance.

To conclude, the Circular provides high-level guidance for LCs in adopting LMs through the introduction of overarching principles that emphasise risk identification, management and mitigation. This demonstrates the SFC's support for technology adoption while maintaining a vigorous regulatory environment for investor protection, which aligns with that of the city's other financial regulators and provides a cohesive governance direction for the city's finance industry. LCs that wish to adopt LMs in their businesses should review and incorporate the Core Principles into their existing regulatory and compliance policies, procedures and internal controls that already apply to their businesses in regulated activities. Finally, LCs are reminded to make a notification to the SFC if they adopt LMs as the adoption of LMs in high-risk use cases is considered by the SC as a significant change in the nature of their business.

As the adoption of AI becomes more widespread and technological advancements become increasingly sophisticated, AI is expected to be utilised for regulated activities which are currently carried out by humans. This evolution raises intriguing questions regarding the regulatory supervision of technology solutions providers – specifically, whether these providers, which LCs rely on for the technology enabling the provision of services constituting regulated activities, will warrant regulatory oversight if the technology they provide from an integral part of an LC's regulated activities.

For further details on how we can assist you, please contact us at: info@wbylawyers.com.hk.

This article is for general information only and is not intended to provide legal advice.

Ben Wong, *Principal*
Kimberly Yeung, *Trainee Solicitor*

© WBY LAWYERS
DECEMBER 2024

---

[1] Please see the link to the SFC Circular:

https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=24EC55

[2] Language models include large language models ("LLMs") and small language models ("SLMs"), which differ in scale, complexity and specificity. LLMs, which may be more commonly known, are larger in scale, more complex and trained on a wider range of data input sources. Whereas SLMs are smaller in scale and less complex but are trained for specific areas. However, the SFC used the term "language model" in the Circular.

[3] Financial Services and the Treasury Bureau, *Policy Statement on Responsible Application of Artificial Intelligence in the Financial Market* (28 October 2024).

[4] Ibid.

[5] Insurance Authority, 'Chatting about Chatbots and AI' (May 2023) <https://www.ia.org.hk/en/legislative_framework/Conduct_in_Focus_Issue_07_(Article_03).html> accessed 17 December 2024.

[6] Hong Kong Monetary Authority, *Consumer Protection in respect of Use of Generative Artificial Intelligence* (19 August 2024).

[7] Hong Kong Monetary Authority, *Generative Artificial Intelligence in the Financial Services Space* (September 2024).

[8] Hong Kong Monetary Authority, *Generative Artificial Intelligence Sandbox* (20 September 2024).

[9] Securities and Futures Commission, *Circular to licensed corporations – Use of generative AI language models* (12 November 2024).