

Hong Kong SFC sets rules for licensed firms using generative AI models

Source copy kept by wheresthe.ai for the story "Hong Kong SFC sets rules for licensed firms using generative AI models" (<https://wheresthe.ai/d/hk-sfc-genai-language-models-circular-2024-11/>).

Source: <https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2024/11/sfc-circular-to-licensed-corporations-on-use-of-generative-ai.html>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: 9e5a520e06dc4987cc474824659ddd901f040d9cd43286bb23c94ec4e8db72fd

SFC's Circular to licensed corporations – Use of generative AI language models

Artificial Intelligence

2 December 2024

The Hong Kong Securities and Futures Commission (SFC) issued its Circular on generative artificial intelligence language models on 12 November 2024. The purpose of the Circular, which is effective immediately, is to provide guidance to licensed corporations (LCs) on compliance with their regulatory obligations in the context of their adoption and use of generative artificial intelligence language models (AI LMs).

The SFC observes that firms are using AI LMs to respond to client enquiries via chatbots, summarise information, generate research reports, feed into investment decision making processes and generate computer code, and states that it encourages and supports the responsible use of AI LMs by LCs. The SFC notes that, while AI has been used in the financial industry for decades, the accessibility of AI LMs, which can accept natural language inputs from users, "democratises" access to AI and lowers barriers to entry for firms – which also increases the risk of deployment without appropriate mitigation and over-reliance by users on "human-like" responses.

A risk-based approach

The Circular flags certain key risks relating to the adoption of AI LMs by LCs:

inaccuracy, bias, unreliability and inconsistency of output, arising from AI LM hallucinations, bias in training and AI LM model performance drift heightened risks of cyberattacks and leakage of confidential information reliance on external service providers to develop and maintain AI LMs.

The SFC confirms that, in implementing the requirements of the Circular, LCs may adopt a risk-based approach, taking measures that are commensurate with the materiality of the risks presented by specific use cases. Providing investment recommendations, investment advice or investment research to investors or clients are *prima facie* high-risk, because problematic outputs may lead to misinformation or the recommendation of unsuitable financial products. The SFC recognises that some LCs may need time to update their policies and procedures to meet the requirements and the SFC will take a pragmatic approach in assessing LCs' compliance with the Circular.

Four core principles

The SFC's guidance is distilled into four core principles:

Senior management responsibilities : an LC's senior management should ensure that effective policies and internal controls are implemented and that there is adequate senior management oversight and governance, by suitably qualified and experienced individuals. This oversight should cover the entire model lifecycle, which includes two key phases model development (i.e., designing and training the model) and model management (i.e., ongoing monitoring of the deployed model). To meet the fit and proper requirement, relevant staff should have competence in AI, data science, model risk management and domain expertise. While the LC can delegate certain functions (e.g., model validation), it remains responsible for ensuring compliance with the relevant requirements.

AI model risk management : LCs undertaking model development should, where practicable, have a development function that is segregated from the function that validates, approves and monitors the model. End-to-end testing of model performance should be conducted, covering the entire process from user input to system output and

related functionality. Once launched, the AI LM should be subject to ongoing review to ensure that it remains fit for purpose. Model development requirements apply where an LC undertakes any activity to develop, customise, refine or enhance an AI LM, including fine-tuning, retrieval augmented generation (RAG), content filtering and integrating external tools, but not where the AI LM merely configures the essential parameters of an off-the-shelf AI LM product (which are, however, subject to the model management requirements). For high-risk uses, the Circular sets out four requirements: (i) model validation and ongoing review to improve factual accuracy; (ii) having a human in the loop to review output before relaying it to the user (although the SFC notes there may flexibility on this requirement depending on the use case); (iii) testing output robustness to prompt variations; and (iv) disclosing to users that they are interacting with AI.

Cybersecurity and data risk management : LCs should keep abreast of the cybersecurity threat landscape relating to AI LMs and have effective policies and controls to manage the risks, including adversarial attacks against the model, e.g., attempts to steal confidential information from model training data or tricking an AI LM to output incorrect responses. LCs should also ensure the quality of the training data, identifying and mitigating biases that may affect the use case, and have regard to existing guidelines on data protection in the context of AI.

Third-party provider risk management : LCs should exercise due skill, care and diligence in selecting third-party providers, including performing appropriate due diligence and ongoing monitoring. Noting that there may be limited transparency and information regarding third-party systems, the Circular requires LCs to assess the extent to which the third-party provider itself has an effective risk management framework (to the extent practicable) and whether the output and performance of the third-party AI LM model are appropriate for the specific use case. LCs should also assess if breaches by the third-party provider of data privacy or intellectual property laws could have a material impact on the use case, and the extent to which the model will be dependent on the consistent delivery and availability of the third-party service and put in place appropriate contingency plans. In the case of open source AI LMs, for which there may be no clear third-party provider on whom to conduct diligence, LCs are nevertheless responsible for ensuring that the model complies with relevant model development and model management requirements.

Notification under the Information Rules

The Circular notes that LCs who intend to deploy AI LMs in high-risk use cases are subject to the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules , which require intermediaries to notify the SFC of significant changes in the nature of their businesses and the type of services they provide. LCs are encouraged to discuss their plans with the SFC as early as possible in the planning and development of the AI LM.

Linkedin

Twitter

Mail