HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

1 November 2019

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

High-level Principles on Artificial Intelligence

The Hong Kong Monetary Authority (HKMA) conducted a survey in Q3 2019 on the use of artificial intelligence (AI) by banks. It is noted that many banks are adopting or planning to adopt AI applications. The scope of AI usage is also expanding from customer-facing services (e.g. chatbots and personalised marketing) to internal processes and risk management areas (e.g. operational automation, cyber and fraud risk management). Details of the survey results will be published very soon.

The growing use of AI presents not only opportunities but also new risk management challenges to banks. The HKMA therefore considers it appropriate to provide guidance to the banking industry on the use of AI applications. The high-level principles set out in this letter have been developed having regard to sound industry practices and similar principles formulated by leading overseas authorities. Banks are expected to take these principles into account when designing and adopting their AI and big data analytics applications. These principles are high-level in nature as the HKMA is mindful that overly prescriptive or rigid requirements may inhibit the further development of AI-related technologies. Banks may apply the following principles in a proportionate manner that reflects the nature of their AI applications and the level of risks involved.

Governance

1. Board and senior management accountable for the outcome of AI applications – Some AI applications have self-learning capabilities from experience and examples (e.g. via reinforcement learning and deep learning) and may be able to make automated decisions on behalf of their banks. The board and senior management of banks should appreciate that they remain accountable for all AI-driven decisions. Accordingly, they should ensure that proper governance framework and risk management measures are put in place to oversee the use of AI applications within their institutions. Moreover, the roles and responsibilities of the three lines of defence in developing and monitoring the operations of AI applications should be clearly defined.

Application design and development

2. Possessing sufficient expertise – Given that designing and developing AI applications requires specific expertise, banks should ensure that their developers have the requisite competence and experience. Senior management should satisfy themselves that there is an effective mechanism to supervise the relevant staff. They should also implement appropriate programmes to recruit, train and retain employees with suitable skillsets.

3. Ensuring an appropriate level of explainability of AI applications – Trustworthy and robust AI applications should be explainable (i.e. no black-box excuse) to all relevant parties. Banks should implement adequate measures during the design phase to ensure a level of explainability which is appropriate and commensurate with the materiality of their AI applications.

4. Using data of good quality – As the accuracy and performance of AI applications depend heavily on the data used to train the AI models, banks should adopt an effective data governance framework to ensure that the data used are of good quality and relevance. For instance, data quality assessment may be performed with respect to AI applications based on appropriately defined data quality metrics (covering factors such as accuracy, completeness, timeliness and consistency of data). Data quality issues identified should be escalated to the responsible parties for rectification in a timely manner.

5. Conducting rigorous model validation – Rigorous validation and testing of trained AI models should be performed to confirm the accuracy and appropriateness of the AI models before they are deployed for production use.

It is preferable to involve an independent party (e.g. the second or third line of defence or an external consultant) in the model validation process.

6. Ensuring auditability of AI applications – There is a need to track the outcome of AI applications on a continuous basis and where necessary gather evidence to support investigations when incidents or unfavourable outcomes arise. Banks should build in sufficient audit logs and produce relevant documentation during the design phase. These audit logs and documentation should be retained for an appropriate period of time to ensure auditing is possible.

7. Implementing effective management oversight of third-party vendors – Where banks rely on third-party vendors to develop AI applications, they should perform proper due diligence on these vendors having regard to the applicable principles set out in this letter. They should also implement effective vendor management controls including periodic reviews of the services provided to manage the associated risks.

8. Being ethical, fair and transparent – Banks should ensure that AI-driven decisions do not discriminate or unintentionally show bias against any group of consumers. The use of AI applications should comply with the banks' corporate values and ethical standards, and uphold consumer protection principles. To provide transparency and thereby increase consumers' confidence in AI-powered services, banks should make clear to the consumer, prior to service provision, that the relevant service is powered by AI technology and the risks involved.

On-going monitoring and maintenance

9. Conducting periodic reviews and on-going monitoring – Since AI applications can learn from live data and their model behaviour may hence change after deployment, banks should conduct periodic reviews (e.g. re-validation of the AI model where appropriate) and on-going monitoring to ensure that the applications continue to perform as intended.

10. Complying with data protection requirements – Considering the data-intensive nature of AI applications, banks should implement effective data protection measures. If personal data are collected and processed by AI applications, banks should ensure that they comply with the Personal Data (Privacy) Ordinance and any other applicable local and overseas regulatory requirements. Where appropriate, sanitised data instead of personally identifiable information

should be used.

11. Implementing effective cybersecurity measures – The use of AI applications may expose banks to new cybersecurity threats. These include, for example, such methods as data poisoning and adversarial attacks, which exploit AI models through data manipulation. Banks should ensure that their security controls can effectively deal with such attacks. They should also keep abreast of and remain vigilant to emerging security threats and the corresponding defence measures.

12. Risk mitigation and contingency plan – Even the most robust AI applications may deliver unintended outcomes. Apart from subjecting their AI-driven activities to appropriate risk-mitigating controls (e.g. human-in-the-loop mechanism, prudent risk limits and sample quality assurance check), banks should implement contingency measures that can promptly suspend AI applications and trigger fall back procedures (e.g. human intervention or conventional processes).

As international regulatory standards and industry developments regarding the use of AI are evolving rapidly, the HKMA will keep the aforementioned principles under periodic review and provide further guidance to banks as and when appropriate. Specifically, the HKMA plans to issue separate guidance on the principles relating to consumer protection aspects involved in the use of AI applications.

Should you have any questions about this circular, please contact Mr Tsz-Wai Chiu on 2878-1389 or Ms Glenda Chung on 2878-8533.

Yours faithfully,

Raymond Chan
Executive Director (Banking Supervision)