中銀香港(控股)有限公司
BOC HONG KONG (HOLDINGS) LIMITED

Administrative Measures for Risk and Compliance Management of Artificial Intelligence Applications (Extract)

Purpose

This Administrative Measures aims to establish a framework for the responsible and ethical use of Artificial Intelligence (AI) within the Group, adopting a risk-based approach to the development, procurement, implementation, and use of AI. In light of the rapid development of AI and its impact on the financial services industry, this Administrative Measures will be revised from time to time to reflect compliance requirements, industry standards, and ethical considerations.

Risk Management Principles for AI Applications

1. Sufficient Expertise and Training

The Group allocates appropriate resources to continuously support and develop AI applications.

2. Explainability of AI Applications

The Group adopts proportionate measures, commensurate with the significance of the AI application, to ensure that an appropriate level of explanation is provided, enabling relevant stakeholders to have a basic understanding of the decisions and outputs generated by AI applications.

3. High-Quality Data Management

The Group uses high-quality data and conducts data quality checks and monitoring to meet data quality requirements, data quality assessment criteria, and other AI-related data standards.

4. Conduct Rigorous Validation

All AI applications must undergo assessment and validation prior to deployment, including evaluations of their accuracy, reliability, robustness, and fairness, to ensure that AI models operate as intended.

5. Auditability of AI Applications

The Group establishes and retains sufficient audit trails and related documentation for AI applications to ensure that their usage and outcomes are subject to ongoing audit and review.

6. Oversight of Third-Party Service Providers

The Group implements effective controls over third-party service providers to ensure that they meet the Group's third-party service provider management requirements and the risk management principles set out in this Administrative Measures.

7. Ethical Conduct and Fairness

The Group complies with the Code of Banking Practice, the Treat Customers Fairly Charter, the principles of financial inclusion, a customer-centric approach, other applicable regulatory requirements and consumer protection principles, as well as the Group's corporate values and ethical standards. AI applications shall not involve activities that violate the Group's corporate values and ethical standards, materially impair customers' ability to make informed decisions or their fundamental rights, cause significant harm to customers, or exploit vulnerable groups.

The Group also establishes key principles governing model algorithms to mitigate risks of discrimination, unfair treatment, or bias against customers, ensuring that AI applications deliver objective, consistent, ethical, and fair outcomes and comply with applicable anti-discrimination laws.

8. Transparency and Disclosure

The Group ensures that users of AI applications or services are provided with appropriate, accurate, and easily understandable disclosures before using such applications or services. Information communicated must be clear and straightforward, providing an appropriate level of transparency, including but not limited to disclosure that the service is powered by AI technology, together with explanations of the purpose and intended use of AI, as well as the associated risks and limitations.

9. Regular Review and Continuous Monitoring

Given the risk of AI models experiencing "model drift" or "model degradation," the Group establishes monitoring tools that are appropriate and proportionate to the level of risk and provides feedback channels for users of AI applications. The Group conducts continuous monitoring through data and/or user feedback, analyzes results in a timely manner, and takes appropriate follow-up actions. In addition to ongoing monitoring of model performance, the Group also performs regular reviews to assess whether model performance continues to meet established standards and compliance requirements.

10. Data Protection

The Group handles data in accordance with its information security policies and administrative measures to ensure compliance with the Personal Data (Privacy) Ordinance (PDPO), relevant codes of practice and practical guidance issued by the Office of the Privacy Commissioner for Personal Data under the PDPO, and other applicable regulatory requirements.

11. Cybersecurity

To address potential malicious cyberattacks against the Group's AI applications, the Group implements appropriate cybersecurity safeguards and defense measures. The Group also closely monitors emerging cyberattack techniques, timely reviews the relevant security mechanisms, and enhances its defenses where necessary.

12. Risk Mitigation and Contingency Plans

The Group implements appropriate risk controls for AI-related activities (e.g., human-in-the-loop controls) and establishes contingency plans for AI applications. Where necessary, the Group may suspend the operation of an AI application and activate fallback procedures.