ICAC

CPAS 防貪諮詢服務 Corruption Prevention Advisory Service

CORRUPTION PREVENTION GUIDE FOR BANKS

- develops an audit programme setting out the auditing assignments to be performed and conducts regular review to the programme taking into account the risk of key business processes; and
- reports directly to the Audit Committee, if established, or the senior management and draws their immediate attention to any significant irregularities detected in the course of audit review.

- Conduct periodic compliance / audit checks to ensure bank staff's compliance with the established policies and procedures.
- Conduct regular/random independent audits on operations/processes/transactions that are exposed to risks of corruption or malpractice (e.g. based on the audit team's knowledge or past corruption cases) to deter and detect irregularities. Deploy management/exception reports and computer-aided audit tools to facilitate the audit. Regularly monitor and review the risks and controls, and update/improve the controls where necessary.
- Make the parties concerned (e.g. bank staff) aware of the random/independent check policy for deterrence purpose.
- Require the Board to give due consideration to the opinions and findings of both the internal and external auditors, and take timely actions in response to the recommendations/findings, as well as monitoring the progress in redressing any problems/loopholes raised by the auditors.

3.3.10 CONTROL THROUGH DIGITALISATION AND REGTECH SOLUTIONS[23]

- Identify and computerise/automate the work processes and workflow management where necessary and practicable, and resources permit, to reduce corruption and malpractices arising from manual errors and human manipulation.
- Upon considering adoption of technologies / Regtech solutions, seek expert advice, keep in view the technological development in the industry, and make reference to the regulator's recommendations where necessary and practicable, among others.
- Build in the necessary functionalities (e.g. the function of generating management and exception reports for management's review and analysis, the function to facilitate electronic declaration of conflict of interest by directors/staff and management of such declarations, monitoring on real time functions, case allocation and monitoring functions, adoption of artificial intelligence to automate business process, detect patterns and general insights) from the system / Regtech development stage to facilitate corruption and fraud prevention or in more holistic terms, overall governance and internal control.

[23] *The HKMA promotes Regtech adoption in Hong Kong in recent years. Banks may refer to relevant webpage of HKMA for details (www.hkma.gov.hk/eng/key-functions/banking/regtech-knowledge-hub/). The term "Regtech" refers to use of technologies (e.g. artificial intelligence, machine learning, natural language processing, optical character recognition) that enhances efficiency and/or the effectiveness of risk management and regulatory compliance.*

- Where a workflow is digitised/automated, install adequate and essential security safeguards (e.g. encryption, data classification) and controls to enhance the effectiveness of digitalisation / Regtech solutions and efficacy of corruption/fraud prevention.
- Ensure effective implementation and usage of information technology (IT) systems / Regtech solutions by staff, covering issuance of clear policies, the requirement for generation of periodic reports for management's review and prudent follow-up, safekeeping of such reports for a specified period, provision of adequate training to staff on the proper usage, etc.
- Conduct periodic monitoring and assessment on systems / Regtech solutions adopted on areas including effectiveness of risk management and security controls regularly after the launch of the systems / Regtech solutions by staff members / external advisors with the necessary competencies and expertise in performing the assessment, who are also independent from the design, implementation and operation of the systems / Regtech solutions.

3.4 CONTROLS AGAINST MONEY LAUNDERING

Corruption and money laundering are very often intertwined. On one hand, money laundering allows the concealment of the unlawful source of funds and assets including proceeds of a corruption offence. Such corrupt proceeds may be placed, layered or integrated into one's legitimate accounts without being detected and confiscated. On the other hand, corruption may also facilitate the commission of a money laundering offence and hinder its detection. In terms of the channels for laundering proceeds for illicit activities, threat analysis reveals that banking sector continues to be exposed to relatively higher risks given that money laundering syndicates often attempt to misuse bank accounts for money laundering, trying to make use of Hong Kong's efficient financial and banking systems[24]. Besides, with technological advancement, the global payment landscape has been developing rapidly. Stored value payment products, internet and mobile payment services have gained popularity, with increased linkages to bank accounts. While bank accounts are the most common vehicle exploited for money laundering (Reference at ***Chapter 4***), money launderers may also attempt to launder their proceeds of illegal acts including corruption through other operations of banks (e.g. wealth management services) to create complex layers of transactions to increase difficulties in tracing the origins of funds (Reference at ***Chapters 5*** and ***6***). To safeguard the integrity of the banking industry and the bank itself against money laundering threat and the related corruption/fraud, banks should implement the following

[24] *The "Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report" published in July 2022 examines the money laundering and terrorist financing threats and vulnerabilities facing various sectors in Hong Kong and the city as a whole. The report is available at www.fstb.gov.hk/fsb/aml/en/doc/2nd%20HK%20ML%20TF%20Risk%20Assessment%20Report_e.pdf.*