Annex

Sound practices for customer data protection

The HKMA completed a round of thematic examinations on customer data protection in 2022. This note sets out the sound practices observed in the thematic examinations.

1. Data governance

Effective data governance and risk management framework – AIs should put in place effective data governance and risk management framework to protect their customer data throughout the data lifecycle in a secure manner. We observed from the thematic examinations that the board and senior management of AIs exercise sufficient oversight of the formulation and implementation of data security strategy covering customer data protection. In particular, the more advanced AIs have established a management committee comprising various representatives from business, risk management and compliance functions to oversee matters related to customer data protection.

Some AIs have established an effective governance framework for customer data protection to ensure the roles and responsibilities of relevant departments and staff (e.g. data owner and three lines of defence) are clearly defined and documented. The customer data governance framework covers processes for evaluating the adequacy and effectiveness of the AIs' control practices such as identity and access management and encryption controls to safeguard customer data against elevated risk of data breach. These AIs also conduct regular assessments to ensure continuous compliance with relevant laws, regulations and their internal policies.

2. Customer data inventory management

Comprehensive customer data inventory – AIs should identify and document the locations of their customer data residing in different parts of AIs' networks, systems and premises, in order to facilitate the prevention and detection of loss or leakage of customer data. Some AIs have developed formal policies and procedures to provide guidance on effective maintenance and updating of the customer data inventory. They maintain comprehensive customer data inventory covering all relevant systems and parties including third parties that process or store customer data. A dedicated responsible officer is assigned to coordinate the annual customer data inventory review exercise. The more advanced AIs use a centralised inventory system for recording and tracking their customer data. This facilitates reviews of the inventory to ensure completeness and accuracy.

3. Controls over transmission and storage of customer data

Robust controls over transmission and storage of customer data – AIs should adopt effective security measures to minimise the risk of data breach when handling customer data in transit, at rest and at end of life. Many AIs have developed data loss prevention (DLP) policies and measures for protecting customer data. These policies and relevant rules of DLP, such as coverage and thresholds for alert and monitoring, are approved by senior management and regularly updated to reflect changing business operations. DLP measures are implemented for internal and external communications (e.g. email, cloud storage service and file transfer protocol). Some AIs have also set up monitoring mechanisms on network traffic to detect suspicious activities.

Proper use of portable storage media – AIs should take effective measures to address the risk of unauthorized downloading of customer data to portable storage media. We observed that AIs have deployed appropriate security controls including strong encryption and restriction on portable storage media to protect the confidentiality and integrity of customer data stored in these media. Some advanced AIs perform testing of customer data protection controls periodically to assess their effectiveness.

4. Physical and logical security controls of customer data

Adequate physical and logical security controls – AIs should implement proper physical and logical security controls to prevent customer data from unauthorized access or theft. We noticed that many AIs have put in place various physical security controls (e.g. surveillance cameras and disallowing use of electronic devices) and multi-factor authentication for premises and systems where massive customer data are processed or stored. In terms of access management, access to information assets such as shared folders containing customer data is granted strictly on a need basis and regularly reviewed. A few AIs have implemented dynamic watermarking on screen or printed documents to deter users from sending customer data to third parties without proper authorization. In addition, some AIs perform periodic security assessments of customer data protection through on-site inspections. These assessments cover areas such as network security, physical and logical access controls of AIs' and service providers' operating environments.