SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

30 March 2023

Circular to licensed corporations

Data risk management

This circular highlights the standards of risk governance[1], controls and monitoring[2] which the Securities and Futures Commission (SFC) expects of licensed corporations (LCs) in their data risk management practices.

Data risk is drawing mounting attention around the globe in light of the burgeoning volume of data collected and used in business operations. In the context of this circular, data risk refers to the risk of operational disruptions and reputational or financial losses due to LCs' inadequacy in managing the data lifecycle, which includes the collection, classification, usage, retention, transfer and disposal of data. Significant data risk incidents have occurred, including inadvertent disclosures of material non-public information and leakage of client data from scrapped hardware or third-party service providers.

Data risk management was a focus of a recent thematic review conducted by the SFC[3]. The report on this review, published today, provides an overview of the industry landscape and current market practices as well as detailed guidance to facilitate LCs' ongoing refinement of their risk management processes[4].

A. Data risk governance

A sound data risk governance framework enables LCs to develop a robust management structure with well-defined roles and responsibilities to address data risks. It also allows LCs to respond promptly to data risk incidents, to ensure compliance with applicable laws and regulations, including the Personal Data (Privacy) Ordinance (Cap 486) (PDPO), as well as to effectively promote staff awareness of data risks.

LCs should beware of control deficiencies which could undermine the effectiveness of their management oversight. These deficiencies, which the SFC observed at some LCs, included not clearly delineating management responsibilities for governing data risks or not defining the escalation protocol and timeframes for the timely reporting of data risk incidents to senior management.

---

1 General Principle 9 and paragraph 14.1 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) and Part I of the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (Internal Control Guidelines).

2 General Principle 3 and paragraph 4.3 of the Code of Conduct and Part IV of the Internal Control Guidelines.

3 The SFC announced its thematic review in a circular issued on 16 November 2018. The review covered LCs' risk management practices in respect of data risks as well as operational and remote booking risks relating to trading activities. A separate circular issued today sets out the regulatory standards the SFC expects of LCs in their operational and remote booking risk management practices.

4 See Section D of the report.

Expected standards

LCs should put in place a sound risk governance framework for the effective management of data risks and compliance with the applicable legal and regulatory requirements[5]. The framework should cover the following areas, amongst others:

(a) clear definition of senior management's responsibilities and accountability[6] for overseeing data risk management; and

(b) structured protocols for handling data risk incidents and reporting them to senior management and relevant authorities (where appropriate) in a timely manner.

B. Data lifecycle controls and monitoring

Appropriate controls and monitoring are essential for LCs to mitigate data risks arising from poor data quality, unauthorised access to data, data leakage and the loss of sensitive data. In particular, controls and monitoring should be instituted in the following areas:

- management of the data lifecycle, namely data collection, classification, usage, retention, transfer and disposal, as elaborated in sub-sections (i) to (v) below; and
- use of third-party service providers, as elaborated in sub-section (vi) below.

(i) Data collection

LCs often collect and process massive amount of data for conducting regulated activities and making business decisions. To mitigate the risk of business disruptions or the adverse effects poor-quality data may have for clients, some LCs performed due diligence on data providers and assessed the reliability of data sources. Some LCs also carried out sample tests to ascertain the accuracy and completeness of critical data collected.

Expected standards

LCs should collect data from reliable sources and take appropriate steps to ensure the quality of the data collected.

(ii) Data classification

Data collected by LCs may bear varying degrees of confidentiality. To mitigate the risks of data loss or leakage, it is common for LCs to classify data into different categories (such as "highly confidential", "confidential", "internal" and "public") and apply stricter data protection measures to more sensitive data.

[5] Including the PDPO.

[6] See the SFC's 16 December 2016 Circular to Licensed Corporations Regarding Measures for Augmenting the Accountability of Senior Management.

Expected standards

LCs should reasonably classify the data they handle based on the level of sensitivity and implement commensurate protection measures.

(iii) Data usage

Controls and monitoring for who has access to data and how data is used are vital to detect and prevent unauthorised usage or leakage of sensitive data such as material non-public information. We observed that LCs often implement data access controls and data flow monitoring mechanisms to ensure appropriate access to and usage of sensitive data.

Expected standards

LCs should ensure that sensitive data can only be accessed, used or modified by authorised parties.

(iv) Data retention

Proper maintenance and retention of data facilitates LCs' business operations and their compliance with applicable regulatory record-keeping requirements. We observed that some LCs clearly specified the minimum periods for which different types of data should be retained. Some LCs which belonged to a global financial group also kept their data offshore as a backup measure.

Expected standards

LCs should establish data retention and backup policies to ensure the safekeeping and availability of data within a specific timeframe to comply with regulatory record-keeping requirements and meet their business needs.

(v) Data transfer and disposal

Data transfer and disposal are processes which bear inherently greater risks of data leakage or loss, particularly when a third-party data recipient or data processing system is involved. To ensure the secure transfer of data, some LCs implemented data encryption, software and hardware installation controls as well as data loss prevention tools. While LCs disposed of sensitive data in designated ways such as paper shredding and media degaussing, some LCs additionally required an independent function (eg, compliance) or a third-party service provider to monitor the data disposal process.

Expected standards

LCs should implement adequate safeguards to prevent data in transit from being leaked to unintended parties and discarded data from being maliciously accessed or recovered.

(vi) Use of third-party service providers

From time to time, LCs may engage third-party service providers to perform various duties along the data lifecycle. To ensure that service providers implement proper safeguards for data protection purposes, some LCs assessed the capability of their service providers (eg, for the secure processing of sensitive data) by conducting initial due diligence and ongoing monitoring of their performance.

Expected standards

Where a service provider is engaged in the data lifecycle, LCs should perform proper due diligence and ongoing monitoring to ensure that the service provider has the capability to safeguard the data and comply with the applicable legal and regulatory requirements.

Should you have any questions regarding this circular, please contact your case officer.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

End

SFO/IS/008/2023